SECURING
FINANCIAL SERVICES

5th July 2023

London

@eCrime_Congress
#securingfinancialservices

#securingfinancialservices

How do you know you are not the weakest link?

Forthcoming events

SECURING
THE PUBLIC SECTOR

13th September 2023
London

SECURING
EDUCATION

19th September 2023
Online

e-crime & cybersecurity
SWITZERLAND

21st September 2023
Zurich

e-crime & cybersecurity
MID-YEAR

19th October 2023
London

e-crime & cybersecurity
SPAIN

24th October 2023
Madrid

SECURING
TRANSPORT

November 2023
Online

e-crime & cybersecurity
NORDICS

1st November 2023
Copenhagen

e-crime & cybersecurity
BENELUX

7th December 2023
Amsterdam

For more information, please visit
akjassociates.com/contact-us

Welcome to this latest edition of Securing Financial Services. You don't need me to tell you about the complexity and scale of the cybersecurity threat to the economy, to critical national infrastructure in general or to financial services in particular. And while the sector has devoted enormous resources to fighting cybercrime and cyber-enabled fraud, the threat remains high.

Just before the latest round of bank instability, a Bank of England systemic risk survey recently polled 65 executives in the UK financial sector, and shows that 74% of respondents deemed a cyber-attack to be the highest risk to the financial sector in both the short and long term, followed closely by inflation or a geo-political incident.

The number of respondents who believe their company is at high risk of attack grew rapidly this year, from 31% in the first half of the year to 62% in the second. Those considering the threat to be low has decreased by 20%, to just 3%. What's more, 83% believe that cyber-risk in the financial sector has increased in the past year.

These are interesting findings because they reveal that while financial institutions do not under-estimate the potential for harm posed by cyber-attacks, they do not believe that the actual, realised damage will be as significant as that incurred from other, bigger picture, business-related threats. To an extent, this assessment is borne out by recent events. Banks are failing not because of cyber-attacks but because of rate rises, poor credit and investment decisions and deeper cultural failings.

So, what type of cyber-incident does pose the most significant threat to financial institutions and the banking system? Central banks worry less about attacks on single institutions and more about attacks on the data that institutions in general rely on; they worry about attacks that could cause bank runs across multiple banks; they worry about single points of failure in the third-party cloud ecosystem.

Ultimately though, the system is only as good as its weakest link. A compromised firm will be connected through an almost infinite web to the rest of the system and so represent a threat to the whole.

So how should banks be strengthening their cyber-defences to make sure that a firm-wide event doesn't become a system-wide event? These are the kinds of questions we will be looking at at today's event as well as hearing about the latest technologies from some of the key providers.

But one of the main aims of our events is to facilitate conversation and dialogue. So please, enjoy your event, and take the opportunity to mingle with peers, colleagues and solution providers. If you have any questions, please do not hesitate to ask any member of the team.

Simon Brady | Editor

@eCrime_Congress #securingfinancialservices

5th July 2023

Park Plaza Victoria
London

SECURING
FINANCIAL SERVICES

Editor:
Simon Brady
e: simon.brady@akjassociates.com

Design and Production:
Julie Foster
e: julie@fosterhough.co.uk

Forum organiser:
AKJ Associates Ltd
4/4a Bloomsbury Square
London WC1A 2RP
e: simon.brady@akjassociates.com

Booklet printed by:
Method UK Ltd
Baird House
15–17 St Cross Street
London EC1N 8UN
e: hello@thisismethod.co.uk

Articles published in this magazine are not necessarily the views of AKJ Associates Ltd. The publishers and authors of this magazine do not bear any responsibility for errors contained within this publication, or for any omissions. This magazine does not purport to offer investment, legal or any other type of advice, and should not be read as if it does.

Those organisations sponsoring or supporting the Securing Financial Services bear no responsibility, either singularly or collectively, for the content of this magazine. Neither can those organisations sponsoring or supporting the Securing Financial Services, either singularly or collectively, take responsibility for any use that may be made of the content contained inside the magazine.

SECURING
FINANCIAL SERVICES

7 key takeaways for financial services from recent research

Best practices to reevaluate risk in your programme.

Akamai reports

Akamai has been publishing the State of the Internet (SOTI) reports ever since we added cybersecurity controls to our platform approximately 10 years ago. The reports have traditionally tackled one topic, such as phishing or API attacks. This time, however, we have taken a much broader approach and cover a number of issues that impact the financial services industry. Some of the topics into which we dove deeply include web application and API attacks, zero-day threats, account takeover (ATO), and phishing trends.

The top 7 insights

Here are the top seven trends we gained from this research:

1. The financial services industry ranks #1 for phishing, #2 for DDoS attacks, and #3 in web app and API attacks.
2. Distributed Denial-of-Service (DDoS) attacks against financial institutions remain steady year-over-year, but attacks are shifting regions, with attacks against EMEA increasing to 73%.
3. The financial services industry shows the highest growth in web application and API attacks with a 3.5x surge.
4. Exploitation of new and emerging vulnerabilities, like the Atlassian Confluence RCE vulnerability (CVE-2022-26134), is found to begin within 24 hours of disclosure and peak quickly.
5. Attackers are focused on customer-related ATO and web scraping-related attacks, as is clearly shown by the 81% growth in bot activities against financial institutions.
6. Phishing attacks target consumers (80.7%) more than business accounts; on the dark web, there is massive demand for consumers' compromised accounts, which are used in fraud-related attacks.
7. Phishing campaigns (like Kr3pto) are introducing techniques that bypass two-factor authentication (2FA) solutions using one-time password tokens or push notifications.

Now, let's take a deeper dive into each insight, and review the best actions to take in response to the current threat landscape to these trends.

1. The financial services industry ranks #1 for phishing

Engage with leadership about how your organisation compares with peers and across industries. Senior leaders and the board often want to know how they compare with other companies and sectors, so this is a good chance to show where the organisation ranks on the attack spectrum.

2. DDoS attacks against financial institutions remain steady

Reevaluate risk profiles based on threats as well as changing regulations like the European Union's Digital Operational Resilience Act (DORA). As the threatscape changes, it is important to validate your risk appetite and acceptance decisions. Do so after a major event or change, or at least annually.

3. The financial services industry has the highest growth in web application and API attacks

Understand your attack surfaces and risk exposures to help you devise mitigation plans. There are two things that always provide great return on investment: (1) increasing situational awareness, and (2) minimising your attack surface. You should think about these two things both internally and externally if you have a matrixed environment.

Consider administering cybersecurity training to employees to raise cybersecurity awareness regionally. In this SOTI report, we observed a 449% surge in web app and API attacks in APJ, which is reflective of the growing number of cyber-attacks in the region.

A recent survey indicated that more than 50% of leaders in Asia think that employees lack the necessary cyber-training or knowledge. We believe that equipping employees with knowledge is a critical part of any first line of defence against such attacks.

4. Exploitation of new and emerging vulnerabilities can begin within 24 hours of disclosure and peak quickly

Have crisis management plans ready to deal with zero-day attacks internally and with third parties. The plans should be tailored based on type; for example, product, protocol, threat, or hardware vulnerabilities. Once you have playbooks for each type of emerging threat then you need to conduct exercises periodically to validate and improve them. These steps will pay dividends by minimising effort and disruption when the next zero-day hits.

The financial services sector's cybersecurity programmes are some of the most mature in the world, but cybercriminals continue to innovate and find ways to revitalise old attack methods.

Evaluate mitigation techniques like app and API protection, web application firewalls, and microsegmentation until patch management can fix the vulnerability.

5. Attackers are focused on customer-related ATO and web scraping-related attacks

Update playbooks, based on factors like speed of attacks being operationalised and volume of threat attempts, and test assumptions about what would trigger threats and the tools needed to mitigate them. As attacks become faster and consume more resources, it is vital to review processes and update where needed.

6. Phishing attacks target consumers more than business accounts

Understand that you are not only protecting the company, but also your customers and their access. This should be explicitly stated in your incident response programme. Typically, security operations centres and threat intelligence teams are very internally focused.

Partner with fraud and other teams to help protect not only employees, but also the customers. You'll want to provide a great customer experience effort for access and security.

7. Phishing campaigns are using techniques that bypass two-factor authentication solutions

Consider adding the Fast Identity Online v2 (FIDO2) standard as a criteria for your security tools requirements. Many of us have a multifactor or two-factor authentication solution in place, but it is important to have a regular review of the threat landscape to validate that the existing solution still meets your leadership's risk appetite.

As always, we support adopting industry best practices and processes such as Cyber Kill Chain, MITRE ATT&CK framework, and NIST 800-207 Zero Trust Architecture.

Five categories of attacks

Let's take a closer look at attack methods. In our 2022 Web Application and API Threat Report, we talked about the three types of campaigns we were seeing (persistent, short burst and big bang). This time, we share a look at individual attackers across Akamai systems tracked via Client Reputation. We found five basic categories of attacks:

1. 42% account takeover (fraud-based attacks)
2. 39% web scrapers (information-gathering attacks)
3. 7% scanning tools
4. 6% web attackers
5. 6% Denial of Service

The last three categories, although lower in volume, are still dangerous and could cause a major impact for individual companies.

Consider these categories as ways to think about evaluating and analysing your threat environment, and measure how well your organisation is set up to deal with each category. This can also be a great format to brief your leadership on what you are defending against.

Summary

The financial services sector's cybersecurity programmes are some of the most mature in the world, but cybercriminals continue to innovate and find ways to revitalise old attack methods. By covering a spectrum of threats, this report provides you with the best practices to reevaluate risk in your programme, and insights to drive your threat intel and exercise teams.

Stay plugged in to our latest research by checking out our Security Hub.

Read Akamai's latest Apps and API Security Report.

Come talk to us today! □

Protecting the identity system is key to operational resilience in financial services

The barrage of attacks against financial services organisations is not likely to abate.

Simon Hodgkinson reports

Financial services organisations have long been a lucrative target for cybercriminals. A Boston Consulting Group report estimated that financial services companies are 300 times more likely to experience a cyber-attack compared with other sectors. Cyber-attackers target banks and other financial services companies because they offer the promise of a big payout: These companies hold a treasure trove of customer data.

As in most industries, attacks on financial services organisations often target the core identity management system, which is Microsoft Active Directory (AD) for 90% of organisations worldwide. Organisations use AD to manage permissions and access to business-essential applications and services. Cybercriminals routinely exploit the security weaknesses of AD – a quarter-century-old technology – to breach financial systems and move laterally through the network, dropping malware that lurks for months before detonating.

Protecting the identity system is key not only to preventing and remediating cyber-attacks but also to ensuring operational resilience over the long haul. The barrage of attacks against financial services organisations is not likely to abate. But organisations that take action to secure the identity system before, during, and after an attack will more likely withstand a breach and quickly resume operations while minimising the impact on revenue, reputational damage, and legal exposure. As an added benefit, a strong identity system defence can help financial services organisations maintain compliance with financial regulations.

Identity system defence is the foundation of a strong security posture

The prevalence of the identity system as a primary attack vector for cybercriminals is now well known.

> Organisations that take action to secure the identity system before, during, and after an attack will more likely withstand a breach and quickly resume operations while minimising the impact on revenue, reputational damage, and legal exposure.

As details emerged about high-profile cyber-attacks such as Maersk, SolarWinds, and Colonial Pipeline, misuse of credentials and privilege escalation became a common thread. In 2021, Gartner analysts reported that the top technique used in breaches was misused credentials. The most recent Microsoft Digital Defense Report stated that the company blocked 34.7 billion identity attacks in one year, from July 2021 through June 2022.

IT and security teams in financial institutions face multiple challenges in adequately protecting the identity system:

- Legacy AD environments are prone to misconfigurations that accumulate over time, leaving security gaps that are time-consuming and cumbersome to address
- Global adoption of online banking, including through mobile devices, has increased the attack surface
- Customers are vulnerable to evolving tactics such as phishing and social engineering

Although the obstacles are significant, financial services organisations can improve their security posture and overall operational resilience by focusing on specific objectives in protecting AD before, during, and after an attack.

BEFORE ATTACK: Assessing vulnerabilities and closing security gaps

AD was not built to withstand current cyber-threats. Many organisations have legacy AD environments with risky configurations that have accumulated over time. Financial services companies can systematically improve their security stance by:

1. Conducting regular vulnerability assessments of the AD environment using solutions that are updated to address current threats
2. Allocating resources to remediate security vulnerabilities, with priority on high-risk indicators of exposure (IOEs) and compromise (IOCs)
3. Ensuring that vulnerability assessments cover on-premises AD and Azure AD, as attacks can start on premises and move to the cloud, or vice versa

DURING ATTACK: Quickly mitigating unwanted or malicious changes

Speed is the critical factor in mitigating malicious activity in the identity system. Malware can move

By protecting the identity system – the gatekeeper to business-critical applications and services – financial services companies can mitigate the risk of a cyber-attack and streamline compliance with industry regulations.

through an organisation so quickly that human intervention is nearly impossible. According to the Microsoft Digital Defense Report, the median time for an attacker to begin moving laterally after initial device compromise is 1 hour, 42 minutes.

Mitigating identity threats requires:

1. Continuous monitoring for new threats across the hybrid AD environment
2. Multidimensional monitoring that uses AD replication stream data in addition to audit logs to catch malicious changes that can bypass traditional monitoring systems
3. Automated rollback of malicious changes to stop fast-moving malware

AFTER ATTACK: Recovering the identity environment to a malware-free state

Although most organisations are understandably focused on resuming business operations as quickly as possible after a cyber-attack, the focus must be on conducting a thorough recovery of the identity system to a malware-free state to avoid the risk of reinfection. Organisations that conduct disaster recovery exercises in an environment that simulates an encrypted production AD environment will be better prepared if a cyber-disaster occurs.

Financial services organisations can lay the groundwork for a swift AD recovery by implementing a solution that:

1. Automates the AD forest recovery process, which reduces recovery time compared with manual processes
2. Provides the ability to recover AD to any hardware – virtual or physical – to avoid delays in hardware procurement and configuration during incident response
3. Recovers AD to a known-secure state and provides post-breach forensics to ensure that malware is eradicated from the environment

In addition to forming the foundation of a sound security strategy, a strong identity system defence can help financial institutions demonstrate compliance with regulatory requirements. As an example, the Financial Conduct Authority (FCA) enforces mandates regarding how institutions within the UK financial sector ensure operational resilience, particularly against the threat of cyber-attacks. One key step toward complying with FCA regulations is ensuring the cyber-resilience of AD because of its critical role in authenticating users and providing access to business-critical applications and services.

The FCA guidance details requirements for institutions to set impact tolerances for important business services, mandating that "firms should set their impact tolerances at the first point at which a disruption to an important business service would cause intolerable levels of harm to consumers or risk to market integrity." The regulations also state that "firms should test their ability to remain within their impact tolerances for each of their important business services in the event of a range of adverse scenarios, including severe but plausible disruption of its operations."

Key actions for ensuring that AD's impact tolerances comply with the FCA guidance include:

- Improving operational resilience by ensuring that AD can be recovered quickly to a known-secure state
- Overcoming configuration drift by identifying and automatically remediating dangerous and malicious changes to AD
- Filling specialist skills gaps by hiring people and implementing technology specialising in AD
- Establishing a 'risk appetite' benchmark to measure your level of acceptable risk regarding vulnerability patching, identifying and addressing indicators of exposure and compromise in AD, and establishing recovery timelines and processes
- Using timely and actionable threat intelligence to protect against emerging threats that target AD

Cyber-threats will continue to increase in frequency and complexity. But by protecting the identity system – the gatekeeper to business-critical applications and services – financial services companies can mitigate the risk of a cyber-attack and streamline compliance with industry regulations. □

For more information, please visit **www.semperis.com**

semperis

RISK LEDGER

Be confidently on top of your supply chain security

Stay on top of incoming regulations

Scale supplier coverage from 5% to 95%

Automate your vendor risk assessment process

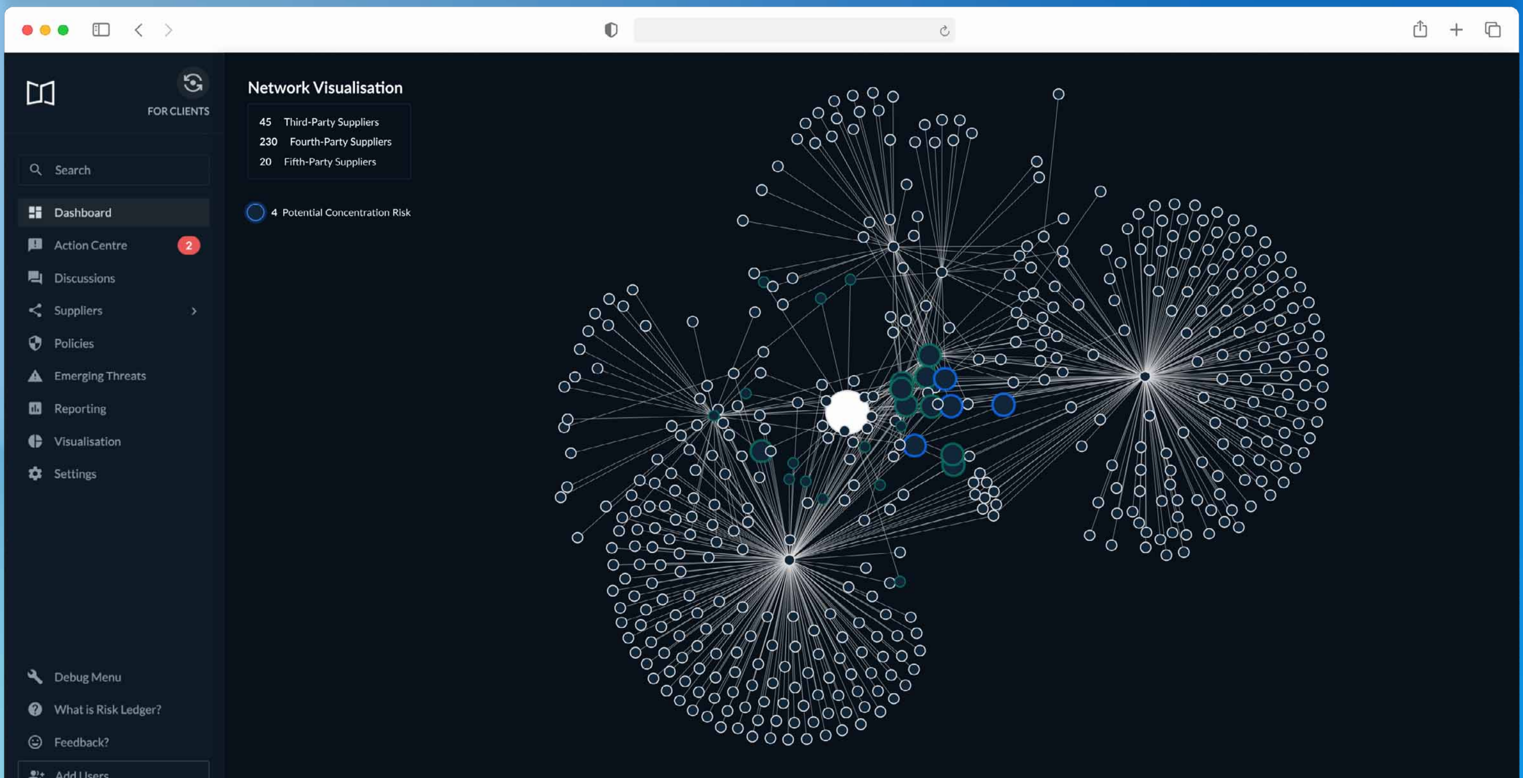
Stay on top of operational resistance requirements

Gain real-time security information on your supply chain

Visualise 4th, 5th & nth parties & identify concentration risks

Join the 3,000 businesses and 12,000 users that are already using Risk Ledger to secure their supply chain security

Simply Business   Quilter   DOMINE DIRIGE NOS   yieldbroker   First Sentier Investors   SUCCESSION WEALTH


Network Visualisation

45 Third-Party Suppliers
230 Fourth-Party Suppliers
20 Fifth-Party Suppliers

4 Potential Concentration Risk

Discovering the ‘unknown unknowns’ of financial services supply chain cyber-risk

Hostile state actors and affiliated hackers are increasingly intent on disrupting the western financial system.

Risk Ledger reports

We are seeing major technological, geopolitical and regulatory changes, which have sped up significantly since the global pandemic and the war in Ukraine, and which have further intensified the cyber-risks to our critical national infrastructure, and the financial services industry in particular. Hostile state actors and affiliated hackers are increasingly intent on disrupting the western financial system. As the New York State Department of Financial Services (NY DFS) rightly warned in the wake of the SolarWinds hack, “the next great financial crisis could come from a cyber-attack.”

While financial services firms commonly have strong cyber-defences in place, not least because of the stringent compliance and regulatory requirements the industry has to meet, there remains a clear weak spot: their supply chains. Financial services companies have seen a 63% increase in cyber-attacks that originated through their supply chains and supply chain attacks have become the second most prominent cyber-threat facing organisations today. Nonetheless, according to recent research, only 40% of organisations say they thoroughly understand their third-party cyber- and privacy risks.

The SolarWinds attack has somewhat driven home the inherent dangers lingering in supply chains. As a direct result of the attack, the NY DFS saw a potentially major threat to the financial system and thus immediately required all New York financial institutions to report any impacts the attack had on them.

While this attack drew a lot of attention because of its massive ‘blast radius’, and because evidence suggests that Russia was behind it, there are hundreds of other attacks against the financial services industry through their supply chains that receive far less attention. For instance, the recent ransomware attack against ION Trading Technologies’ cleared derivatives unit. The attack, which forced ION to take its systems offline, resulted in financial institutions suddenly having to manually confirm trades, causing ripple effects and reporting delays across the sector.

While financial services firms commonly have strong cyber-defences in place, not least because of the stringent compliance and regulatory requirements the industry has to meet, there remains a clear weak spot: their supply chains.

Why financial services are highly vulnerable to supply chain attacks

The industry’s strong dependency on interoperation with often thousands of suppliers, clients, intermediaries and other organisations that they share information with or whose services or systems they use, means that IT security but also procurement and compliance teams face an arduous task in trying to secure their unwieldy supply chains.

The task is further complicated by the major digital transformations that the global economy, including financial institutions, are currently undergoing. As a major European Central Bank’s Banking Supervision research into the digital transformation of the financial services sector has revealed, 90% of financial institutions are making increasing use of APIs and cloud computing as the foundation for their digital transformation strategies. 60% of banks now use AI in their services and operations, including for chatbots, credit scoring and algorithmic trading. These innovations, while essential to boost productivity and growth, also mean a continuously growing dependence on often less cyber-mature Fintech companies and other suppliers.

The ‘unknown unknowns’ of supply chain risks

But if the risks emanating from immediate third-party suppliers would not be difficult enough to manage, there is an entire additional layer that very few organisations are aware of, namely the risks further down their supply chains, from 4th, 5th and 6th parties, and even beyond.

Dan Jones, risk manager in the group sourcing and supply chain management team at Lloyds Banking Group, told a recent CIPS Supply Management Forum that “never before have supply chains been such a high-profile risk, and supply chain resilience is top of the agenda with our regulators and our senior execs”, as well as adding that “to identify ‘fourth-party’ risk had proved invaluable”.

Without greater awareness of what is happening further down the supply chain, it becomes almost impossible to anticipate potential threats that might suddenly surface at 4th, 5th or 6th parties and beyond.

And this is exactly the point. Without greater awareness of what is happening further down the supply chain, it becomes almost impossible to anticipate potential threats that might suddenly surface at 4th, 5th or 6th parties and beyond, but then ripple up and come to affect a financial services client directly. These broader supply chain risks, and the current general lack of visibility into them, remain a serious problem.

Identifying concentration risks to enhance your operational resilience

Apart from extensive manual surveys, there are really only two ways your organisation can currently achieve significant breakthroughs with regard to gaining greater visibility across your entire supply chain, and thus a more in-depth understanding of existing risks. The first is by using a data mapping tool that pulls together data from the open web to try and infer what your supply chain might look like.

The second option is to use a platform like Risk Ledger. Risk Ledger's approach is based on creating a network of clients and suppliers all working together to Defend-as-One® through its platform, which provides clients not only unparalleled and continuous insight into their direct suppliers' security posture, but also deep visibility into the relationships and risks beyond third parties. This allows organisations to understand where they sit within the wider supplier ecosystem, how different security incidents may impact their organisations, given those interdependencies, and where concentration risks might lie.

During a Cyber Innovation Challenge, led by the City of London and Microsoft, a tier-1 bank used Risk Ledger to uncover potential blindspots, and within 48 hours was able to identify 36 fourth parties connected to 14 direct suppliers, 175 fifth parties, 15 sixth parties, and 27 seventh parties, as well as, most important of all, 7 potential concentration risks.

Operational resilience has been on everyone's mind, not least since the Bank for International Settlement's Basel Committee on Banking Supervision published its *Principles for operational resilience* (the POR) in 2021. Identifying concentration risks in your wider supply chain should be a key component of enhancing your operational resilience. This means finding out who the key organisations are in the wider financial sector supply chain ecosystem that are so important (based on interdependencies) that if they were to have a major cybersecurity incident, this would not just affect a few of their immediate clients, but could ripple up the supply chain and directly affect not only your organisation, but potentially even the wider industry.

With this new visibility into an ever-growing threat surface, you have the information and opportunity to collaborate with your internal risk and resilience team(s), and the high-risk suppliers you were able to identify, to address and reduce these risks and demonstrate to regulators that effective risk awareness is guiding your security governance and operational resilience efforts.

If you want to learn more about how to identify and address risks in your wider supply chain ecosystem, including concentration risks, drop by the Education Seminar "How concentration risk in your supply chain affects operational resilience and what to do about it.", facilitated by Risk Ledger's Chief of Staff, Emily Hodges, at the conference on Wednesday, 5th July. □

For more information, please visit
riskledger.com

RISK LEDGER

Cyber-risks lurking within enterprise SaaS apps

Unveiling hidden risks.

AppOmni reports

Data breaches experienced by CircleCi, LastPass, and Okta all share a commonality: the SaaS-to-SaaS connections of these industry-leading apps can be at serious risk for compromise.

And with the average organisation using over 100 SaaS apps, this poses a significant gap in SaaS security, especially if those apps are unsanctioned by IT. This gap is more glaring considering that SaaS security spend often falls short compared to investments in cloud infrastructure protection and network security.

How SaaS apps' allure may lead to IT oversight

As productivity tools for work tasks shift from installed software to SaaS, so too are end-users' behaviours, and employees will always seek ways to increase their efficiency with tools of their preference. Although this behaviour isn't new or malicious, it can create security risks.

Before, organisations added endpoint security to work machines and devices to monitor if their employees downloaded harmful software or if their accounts were compromised. But this strategy doesn't align with how people work today, which is often outside of corporate networks and using personal devices.

Instead of seeking Security or IT approval for onboarding new SaaS solutions, which may result in red tape, delays, or denial, they pull out their credit card or opt for a free trial. Employees seldom consider shadow IT risks when connecting apps to their enterprise SaaS systems such as Microsoft 365 or ServiceNow.

These connections, combined with the users' inherited permission settings, could access an organisation's sensitive data, without being monitored or detected.

The role of OAuth Tokens in SaaS Apps inheriting permissions

SaaS apps (and SaaS-to-SaaS connections) leverage OAuth access tokens from the start of their connection and throughout their lifecycle.

> Before, organisations added endpoint security to work machines and devices to monitor if their employees downloaded harmful software or if their accounts were compromised. But this strategy doesn't align with how people work today.

An SSPM solution's continuous monitoring capabilities helps Security teams determine a baseline of SaaS activity to use as a time-in-point frame of reference. Although chances of a SaaS-related breach won't ever be completely eradicated, an SSPM significantly reduces that risk.

Figure 1: A breakdown of how an SaaS-to-SaaS connection interacts with an OAuth token

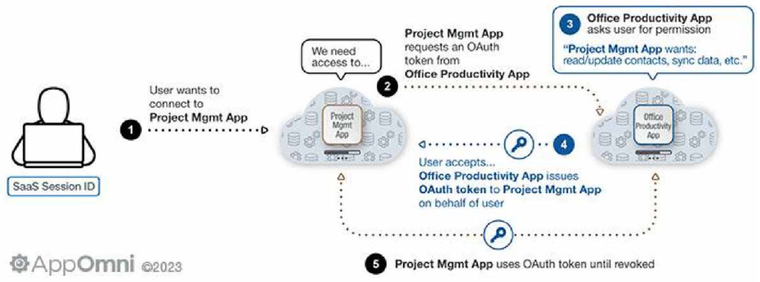

SaaS Session ID
1 User wants to connect to Project Mgmt App
We need access to...
Project Mgmt App
2 Project Mgmt App requests an OAuth token from Office Productivity App
3 Office Productivity App asks user for permission
"Project Mgmt App wants: read/update contacts, sync data, etc."
Office Productivity App
4 User accepts... Office Productivity App issues OAuth token to Project Mgmt App on behalf of user
5 Project Mgmt App uses OAuth token until revoked
AppOmni ©2023

Figure 1 above displays the usual process of this OAuth connection.

Although application tokens provide the user with easy access to the SaaS app, the tokens are valuable for attackers seeking an easily exploitable entry point into an enterprise SaaS system.

The risks of SaaS apps and SaaS-to-SaaS connections

Malicious actors can access CRMs, code repos, and more if they successfully seize OAuth tokens. It's nearly impossible for Security and IT teams to independently manage enterprise SaaS platforms, let alone unauthorised SaaS apps. AppOmni research shows that:

- The average enterprise organisation has 42+ distinct SaaS-to-SaaS apps connected into live SaaS environments. Roughly 50% of these apps weren't connected by IT teams, but by end-users.
- Nearly half of those 42 connected apps haven't been used in the last six months yet still have their data access rights.
- Several of these organisations have almost 900 user-to-application connections.

Without adequate SaaS security, it's difficult to monitor the amount of 'authorised' apps in contact with potentially sensitive data, making connected SaaS apps potential vulnerable blindspots (see Figure 2).

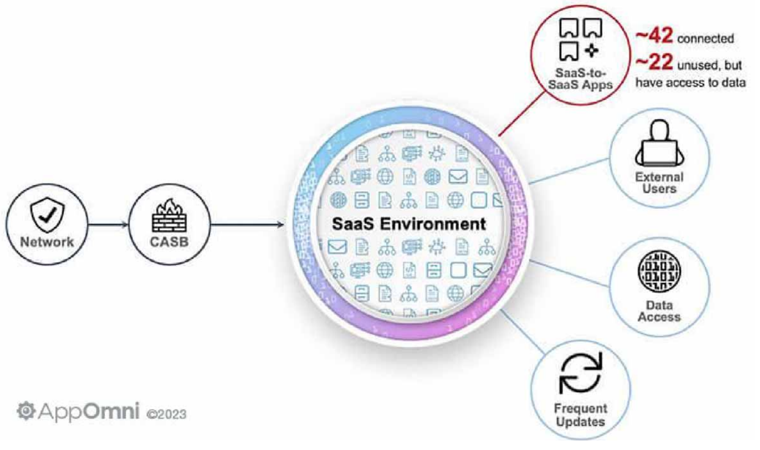
Leverage SSPM for SaaS ecosystem protection

Insufficient SaaS security tooling can hinder Security teams' capacity to gain visibility into SaaS connectivity and the associated user activity. To address these concerns SaaS Security Posture Management (SSPM) solutions provide visibility and control over the SaaS estate.

A Security professional can use SSPM to detect and address any suspicious findings in Salesforce and its connected SaaS apps, reducing attack surface risk and enabling proactive security control.

An SSPM solution's continuous monitoring capabilities helps Security teams determine a baseline of SaaS activity to use as a time-in-point frame of reference. Although chances of a SaaS-related breach won't ever be completely eradicated, an SSPM significantly reduces that risk. □

Figure 2: SaaS environments contain many entry points outside traditional network and CASB protection



For more information, please visit **appomni.com**

AppOmni

eSENTIRE

Build Cyber Resilience Today: Protect Your Business

With cyber threats on the rise, it's crucial to have the right tools and practices in place to anticipate, withstand, and recover from the most sophisticated cyberattacks.

By shifting to a cyber resilience mindset, you can effectively reduce your organisation's cyber risks without straining your security team. Start by:

- Implementing a Phishing and Security Awareness Training program
- Adopting a comprehensive Vulnerability Management program
- Engaging a 24/7 multi-signal Managed Detection and Response (MDR) provider

Learn more about how you can build a more resilient security operation today.

How to increase cyber-resilience in your organisation

Cyber-threat actors are evolving their tactics, techniques, and procedures.

eSentire reports

As the attack surface continues to grow across on-premises, cloud, or hybrid environments, so does cyber-risk. Unfortunately, many businesses are not only ill-equipped to secure their corporate environment, but security leaders also don't have the resources or cybersecurity budgets to maintain deep visibility across their environment – and threat actors are taking note.

While most successful cyber-attacks result in ransomware attack deployment, data compromise or exfiltration, and disruption of business operations, cyber-threat actors are evolving their tactics, techniques, and procedures (TTPs) to gain Initial Access into your networks. Adversaries are using email thread hijacking techniques to conduct phishing and business email compromise (BEC) attacks and SEO poisoning techniques for drive-by social engineering cyber-attacks to lure victims into executing malicious code.

Moreover, eSentire's Threat Response Unit (TRU) has also observed the rise of Initial Access brokers – specialised cybercriminal groups that specifically develop malware designed to gain Initial Access into your environment and providing that access as a service to other cybercriminals.

As a cybersecurity leader, it's more important than ever to ensure your organisation has a strong cyber-resilience strategy as a foundation for your cybersecurity programme so you can defend your organisation against the most critical cyber-threats and reduce your overall cyber-risk.

What is cyber-resilience?

According to the National Institute of Standards and Technology (NIST), cyber-resilience is your "ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber-resources".

> As a cybersecurity leader, it's more important than ever to ensure your organisation has a strong cyber-resilience strategy as a foundation for your cybersecurity programme so you can defend your organisation against the most critical cyber-threats and reduce your overall cyber-risk.

Therefore, your cyber-resilience strategy should account for the full spectrum of your cybersecurity posture, not just the preventative measures to have in place. Your business must be able to:

- *Anticipate cyber-threats:* Your team should be able to keep on top of the latest TTPs adversaries are using, understand how ongoing geopolitical tensions can impact cybercrime, and how threat actors can take advantage of the current macroeconomic climate to launch cyber-attacks. Anticipating cyber-threats also means your team needs 24/7 ongoing security event monitoring, proactive threat hunting capabilities, and deep visibility across your entire attack surface – no matter where your data and users reside.
- *Withstand cyber-attacks:* Today, ransomware attacks or data breaches are no longer considered 'hypothetical scenarios' to be used in tabletop or war game exercises; they are very real possibilities that can cause significant damage to your businesses by disrupting operations, service delivery, and more. Therefore, you must be confident in your ability to not only withstand a cyber-attack, but defend your organisation against an ongoing attack, in real-time to limit its impact. Unless you have 24/7 threat detection and response capabilities, withstanding cyber-attacks may be incredibly challenging.
- *Recover from cyber-attacks:* If your organisation does suffer a cyber-attack that's eventually contained and remediated, it doesn't mean the work is over. Recovering from a cyber-attack is a long and costly process that includes delivering lessons learned to your senior leadership team and the board, conducting digital forensics and incident response to collect evidence for any legal proceedings, conducting a deep post-breach analysis, and more.
- *Adapt to, and keep up with, the evolving threat landscape:* Lastly, as part of your cyber-resilience efforts, you have to work with your business leaders to implement the processes, policies, and technologies required so your organisation can continuously adapt to the threat landscape

(e.g., shifting geopolitical tensions, changes in the macroeconomic climate, etc.)

What are the challenges to achieving cyber-resilience?

As you begin, and develop, your cyber-resilience journey, some challenges you might experience are:

- *Strained cybersecurity budgets* that limit your team from leveraging the best tools, technologies, and resources you need to withstand and recover from a cyber-attack.
- *Lack of skilled in-house cybersecurity* expertise needed to keep up with the expanding attack surface and the resources to retain that expertise.
- *Lack of threat detection and response capabilities* required to hunt, investigate, and proactively respond to cyber-threats 24/7.
- *Lack of deep visibility across the entire attack surface* so your team can protect your most critical data assets and users, wherever they reside.
- *Not being able to get buy-in* from your senior leaders or your peers to implement the policies, protocols, and controls needed to manage and reduce your cyber-risk effectively.

Recommendations to increase your cyber-resilience

Increasing cyber-resilience against phishing scams and business email compromise attacks

Phishing and business email compromise (BEC) attacks continue to be one of the most common ways for cybercriminals to gain access into your IT environment. In our Disrupting Initial Access threat intelligence report, TRU noted that in 2020, email accounted for 66% of all incidents we saw in customer environments and though its use decreased in 2021, we saw a resurgence of email-based malicious code ('malcode') in 2022. To address this, we recommend:

- *Leveraging a Phishing and Security Awareness Training (PSAT) program* to educate your employees on the latest TTPs used by cybercriminals, learn to identify the tactics and techniques being used, and drive behavioural change. The goal with PSAT programmes is not to turn your employees into security experts, but to increase their risk awareness.
- *Implement password security policies* that enables your employees to change their passwords for all their corporate accounts every 60–90 days.
- *Enable the use of multi-factor authentication (MFA)* to limit the impact of credential stuffing attacks. It's important to note that MFA isn't a perfect defence tool and shouldn't be treated as such. Cybercriminals have used MFA fatigue and prompt bombing attacks to bombard victims with MFA push notifications and trick them into authenticating the login attempts.
- *Establish a zero-trust architecture* to verify and limit user access to data that's required at any given specific time. Continually review your access permissions and don't over-provision.

Increasing cyber-resilience against ransomware attacks and zero-day threats

As ransomware attacks become less opportunistic and more highly targeted, it's critical to have the right expertise and resources to prevent your business from disruption. Therefore, we recommend:

- *Adopting a comprehensive vulnerability management programme* that enables continuous awareness of the threat landscape, proactive vulnerability scanning to understand which systems are inadvertently exposed, and disciplined patch management.
- *Partnering with a 24/7 multi-signal MDR provider* for deep visibility across your entire attack surface and 24/7 threat detection, investigation, and response capabilities to identify, contain, and respond to threats that bypass traditional security controls.
- *Leveraging a team of highly skilled threat hunters* with the expertise to develop original threat intelligence and research that continually enhances endpoint policy and protection to eliminate known and unknown cyber-attacks, even those that leverage existing trusted applications for malicious purposes.
- *Engaging a Digital Forensics and Incident Response (DFIR) partner* who can react with industry-leading speed and efficacy, and brings rapid control and stability to your organisation when a breach occurs. When responding to a critical cyber-threat, speed is of the utmost necessity so be sure to consider a DFIR partner who can get you back to normal business operations in a matter of hours, anywhere in the world.

Given the challenges that every security leader is up against amidst the ongoing geopolitical tensions and a burgeoning recession, it's more important than ever to ensure your organisation is as prepared as possible to anticipate, withstand, and recover from a cyber-attack. An effective cyber-resilience strategy will undoubtedly help you make the most of your limited security resources and IT spend in the next year without leaving your organisation exposed to cyber-threats.

DATE FOR YOUR DIARY

SECURING FINANCIAL SERVICES

25th January 2024
London

For more information, please visit
akjassociates.com/contact-us

Sponsors and exhibitors

Akamai | Strategic Sponsor

Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences – helping billions of people live, work, and play every day. Akamai Connected Cloud, a massively distributed edge and cloud platform, puts apps and experiences closer to users and keeps threats farther away.

Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on Twitter and LinkedIn

Semperis | Strategic Sponsor

Semperis is the industry's most comprehensive identity threat detection and response (ITDR) platform for Active Directory and Azure AD.

For more information, please visit www.semperis.com

AppOmni | Education Seminar Sponsor

AppOmni is the leader in SaaS security. AppOmni provides unprecedented data access visibility, management, and security of SaaS solutions, enabling organisations to secure mission-critical and sensitive data. AppOmni's patent-pending technology deeply scans APIs, security controls, and configuration settings to evaluate the current state of SaaS deployments and compare against best practices and business intent.

With AppOmni, organisations can establish rules for data access, data sharing, and SaaS-to-SaaS applications that will be continuously and automatically validated. The company's leadership team brings expertise and innovation from leading SaaS providers, high-tech companies, and cybersecurity vendors. Backed by Cisco Investments, Salesforce Ventures, ServiceNow Ventures, Scale Venture Partners and more, AppOmni was recently named as a PURE CYBER 100 'Companies To Watch In 2023' and one of CyberTech 100's Companies for 2022.

For more information, please visit appomni.com

eSentire | Education Seminar Sponsor

eSentire, is the authority in managed detection and response. The company's mission is to hunt, investigate and stop cyber-threats before they become business disrupting events. Combining XDR technology and 24/7 threat hunting, eSentire mitigates business risk, and enables security at scale. eSentire provides managed risk, MDR and IR services.

For more information, please visit www.esentire.com

Hackuity | Education Seminar Sponsor

Hackuity gives you a complete view of your cyber-exposure depth and tools to interpret it, so you can detect, predict and protect yourself from cyber-vulnerabilities.

For more information, please visit www.hackuity.io

Hoxhunt | Education Seminar Sponsor

Hoxhunt is a global leader in human risk management. The innovative Hoxhunt AI driven human risk platform scales your security culture and behaviour change that enables people to detect and report cyber-attacks that have bypassed your technical security layers, reducing the risk to organisations from sophisticated cyber-attacks targeting humans. Leading organisations of all sizes, including Bird & Bird, Airbus, Docusign, IGT, Nokia and Qualcomm all rely on Hoxhunt for their human risk management solutions that mitigate their most critical risks across email, cloud, social media, and the web.

For more information, please visit www.hoxhunt.com

Illumio | Education Seminar Sponsor

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber-disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centres, and endpoints, enabling the world's leading organisations to strengthen their cyber-resiliency and reduce risk.

For more information, please visit www.illumio.com

KELA | Education Seminar Sponsor

An award-winning cyber-threat intelligence firm, KELA's mission is to provide 100% real, actionable intelligence on threats emerging from the cybercrime underground, to support the prevention and neutralisation of digital crimes. Our success is based on a unique integration of our proprietary automated technologies and qualified intelligence experts. Trusted worldwide, our technology infiltrates hidden underground places and thoroughly monitors, hunts, and mitigates digital crimes to uncover real risks and allow proactive protection. KELA's revolutionary solution arms you with highly contextualised intelligence, as seen from the eyes of attackers, thus enabling the elimination of blind spots and proactive network defence.

For more information, please visit www.kelacyber.com

Obsidian Security | Education Seminar Sponsor

Obsidian Security is the first truly comprehensive threat and posture management solution built for SaaS. Our platform consolidates data across core applications to help your team optimise configurations, reduce over-privilege, and mitigate account compromise and insider threats. The company was founded in 2017 by industry experts from Carbon Black and Cylance including Ben Johnson, Glenn Chisholm and Matt Wolff. Notable Fortune 500 companies trust Obsidian Security to secure SaaS applications, like Salesforce, Workday, Microsoft 365, ServiceNow, Google Workspace and Github. Headquartered in Southern California, Obsidian Security is privately-held and backed by Menlo Ventures, IVP, Greylock, GV, Norwest Venture Partners, and Wing.

For more information, please visit www.obsidiansecurity.com

SECURING
FINANCIAL SERVICES

Ontinue | Education Seminar Sponsor

Ontinue is on a mission to be the most trusted, 24/7, always-on security partner that empowers customers to embrace the future by operating more strategically and with less risk. Grounded in an intelligent, cloud-delivered SecOps platform, Ontinue offers superior protection that goes well beyond basic detection and response services.

Ontinue is the only MDR provider that leverages AI-driven automation, human expertise, and the Microsoft security platform to continuously assess and protect your environment and advance your security posture for digital transformation.

Continuous protection. Always-on prevention Services. Nonstop SecOps. That's Ontinue.

For more information, please visit www.ontinue.com

Risk Ledger | Education Seminar Sponsor

Did you know 60% of organisations have suffered a security breach through a third party? It's understandable – the traditional processes are broken. Organisations face a burden of ineffective, inefficient admin. 'Point in time' cybersecurity assessments make for poor-quality data that goes out of date fast, offering little protection. Risk Ledger helps organisations get their cybersecurity risk assessment tasks done in hours, not days and scale their supplier coverage from 5% to 95% so they can spot more vulnerabilities at just 10% of the cost.

The NHS used Risk Ledger to identify a situation where several third-party suppliers were all dependent on the same fourth-party supplier. They then worked with those third parties to firstly understand that risk, then take action to mitigate it.

With help from insights like this, many of our customers have improved their supplier contracts. Interested in learning more?

For more information, please visit riskledger.com

iZOOlogic | Networking Sponsor

iZOOlogic is a specialist IT security vendor providing threat intelligence and digital risk protection solutions. The iZOOlogic platform is an integrated suite of solutions allowing real-time intelligence into the online threat landscape and provides a seamless global incident response. iZOOlogic protects hundreds of the world's leading brands, across banking, finance, and government from cybercrime.

For more information, please visit izoologic.com

JupiterOne | Networking Sponsor

For more information, please visit www.jupiterone.com

SECURING
FINANCIAL SERVICES

Wavenet | Networking Sponsor

Formed in 2000, Wavenet has grown to become a respected, multi-award-winning provider of telecoms and technology solutions to thousands of businesses and enterprises across the UK.

Wavenet is a managed service provider and has longstanding partnerships with some of the top technology providers on the planet. They provide the legal and financial sector with tailored connectivity, communications and IT solutions as well as CyberGuard; Wavenet's specialist CREST accredited cybersecurity division that provides a full range of IT security services from its 24/7 UK Security Operations Centre.

As a technology partner, Wavenet keep an eye on the future. Planning, adapting, and empowering you to make your organisation brilliant, through their range of core services.

For more information, please visit www.wavenetuk.com

Egress | Branding Sponsor

Egress makes digital communication safer for everyone. As advanced and persistent cybersecurity threats continue to evolve, we recognise that people get hacked, make mistakes, and break the rules. Egress's Intelligent Cloud Email Security suite uses patented self-learning technology to detect sophisticated inbound and outbound threats, protect against data loss, resulting in the reduction of human activated risk.

Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York, and Boston.

For more information, please visit www.egress.com

ThreatLocker | Branding Sponsor

ThreatLocker® is a leader in endpoint security technologies, providing enterprise-level cybersecurity tools for the Managed Services Provider (MSP) industry, to improve the security of servers and endpoints. ThreatLocker's combined Application Allowlisting, Ringfencing™, Storage Control, Elevation Control, and Endpoint Network Access Control (NAC) solutions are leading the cybersecurity market towards a more secure approach of blocking the exploits of unknown application vulnerabilities.

To learn more about ThreatLocker®, please visit www.threatlocker.com

SECURING FINANCIAL SERVICES

AGENDA

08:30	Registration and networking break
09:20	Chairman's welcome
09:30	**Managing security in an ever-evolving supply chain** **Dom Lucas,** Head of Security, British International Investment • Who are the heroes and who are the villains: the broader third-party ecosystem – regulators, clients and interested parties • Evolving the assurance model – it's not always about technology • Considerations for the future
09:50	**Help drive down financial fraud with insightful API security** **Richard Meeus,** Director of Security Technology and Strategy – EMEA, Akamai • What are best practices for managing, governing, and securing APIs? • How can financial institutions gain visibility into their API estate and detect threats or abuse in their APIs? • How can API security help financial institutions detect and remediate fraud before it impacts the business?
10:10	FIRESIDE CHAT **How to measure the value of your technology risk management programme?** **Ash Hunt,** CISO, Apex Group; **Luke Hebbes,** Director of Business Information Security, London Stock Exchange Group (LSEG) • What is the right amount of data to model a technology risk? • How do I know my controls are reducing loss exposure? • How can I articulate the link between risk reduction and business growth to the board?
10:30	**Education Seminars | Session 1** — **See pages 24 to 26 for more details** AppOmni **SaaS is the new business OS. How to harden SaaS apps at scale** **Brandon Romisher,** VP International, AppOmni eSentire **How to improve cyber-resilience in your organisation** **Andy Lalaguna,** Senior Solutions Architect, eSentire Hoxhunt **From war stories to human threat detection** **Petri Kuivala,** Strategic Advisor, Hoxhunt
11:10	Networking break
11:40	**Cyber-risk – boardroom concern, or compliance burden?** **Phillip Hodgins,** CISO, Pension Insurance Corporation • The benefits of cyber-risk understanding at board level • The benefits of non-competitive cross-sector collaboration • The competitive advantages of effective cyber-risk management
12:00	**Stories from the trenches – identity & incident response** **David Hitchen,** Senior Solutions Architect, Semperis • In the aftermath of an identity attack that compromises Active Directory, how can you quickly recover and restore trust in AD? • Hear real-world examples that illustrate how you can perform attack forensics without alerting the attacker, build a defence, recover Active Directory, and make AD more resilient to compromise in the future • Learn the simple steps that your organisation can take to improve your Active Directory security posture and protect AD against today's widespread cyber-threats
12:20	**An enterprise guide to using large language models (ChatGPT, Github Co-Pilot, etc) securely** **Emmanuel Dahunsi,** Security Architect EMEA, Goldman Sachs • What are the major risks of ChatGPT & other LLMs to your organisations? • What security controls & best practices should you consider? • What are large language models (LLMs) and what are the benefits to your organisation?

AGENDA

SECURING FINANCIAL SERVICES

12:40	**Education Seminars | Session 2**		**See pages 24 to 26 for more details**
	KELA Group **From initial access to ransomware attack** **Dave Gill,** EMEA Channel Director, KELA Group	Obsidian Security **SaaS ransomware – How old threats are migrating to the new SaaS landscape** **Chris Fuller,** Principal Product and Solutions Architect, Obsidian Security	Ontinue **Using Microsoft Teams & AI for effective SecOps collaboration** **Drew Perry,** Chief Innovation Officer, Ontinue
13:20	Lunch and networking break		
14:20	**The cybersecurity insurance market**		
	Archie Ghinn, Account Executive – Technology and Cyber Practice, Gallagher • Current market trends • The growing problem: tracking technologies • The interconnectedness of exposures • Getting the right cover		
14:40	**From strength to success: Creating a winning security team for a competitive edge**		
	Ryan Virani, Head of UK&I – Cybersecurity Recruitment, Adeptis Group • Current market trends • Is there really a skills shortage? • Why do people leave their roles? • Are you being paid and paying enough? • Ironing out the challenges in your search process • Retention and upskilling		
15:00	**Education Seminars | Session 3**		**See pages 24 to 26 for more details**
	Hackuity **The magic of the Vulnerability Operation Centre (VOC) applied to risk management in banking and finance** **Sylvain Cortes,** VP Strategy, Hackuity	Illumio **From digital laggard to cybersecurity leader** **Raghu Nandakumara,** Senior Director – Solution Marketing, Illumio	Risk Ledger **How concentration risk in your supply chain affects operational resilience and what to do about it** **Emily Hodges,** Chief of Staff, Risk Ledger
15:40	Networking break		
16:10	**EXECUTIVE PANEL DISCUSSION**	**Senior leadership discussion**	
	Peter Smith, CISO, Allica Bank; **Guillaume Ehny,** CISO, Kroo; **Jill Robertson,** Head of Information Security Change, Metro Bank; **Matt Adams,** Security Architect, Santander • Integrating cybersecurity into wider enterprise risk management frameworks • Becoming a more strategic partner to the business? • Building resilience against third-party security threats • Web 3.0 and the next generation of the internet: securing new technologies and services		
16:50	Chairman's close		
17:00	Drinks reception		
18:00	Conference close		

Education seminars

Throughout the day a series of education seminars will take place as part of the main agenda. Delegates will be able to choose to attend any of the seminars, all of which will provide vendor-neutral, hands-on advice. Seminars within each session run concurrently.

Session 1: 10:30–11:10

AppOmni

SESSION 1
10:30–11:10

SaaS is the new business OS. How to harden SaaS apps at scale

Brandon Romisher, VP International, AppOmni

Today's SaaS apps are complex platforms, endlessly configurable and integrated everywhere in order to power internal and externally facing business processes. When it comes to securing SaaS, it's all about your config, but security is flying blind and with limited subject matter expertise. How do you harden access controls, ensure correct RBAC constructs and permissions assignments, identify risky 4th party connected apps, monitor high-risk users and detect security events?

In this session, you'll learn

- How FS companies of all shapes and sizes are using AppOmni to automate SaaS security, at scale

eSentire

SESSION 1
10:30–11:10

How to improve cyber-resilience in your organisation

Andy Lalaguna, Senior Solutions Architect, eSentire

In today's threat landscape, security leaders must shift their focus to improving their cyber-resilience. The ability to anticipate, withstand, recover from, and adapt to the evolving cyber-threats will dictate how well-equipped your cybersecurity programme is at defending against these threats. However, given the lack of skilled in-house security resources, it can be challenging to balance the number of incoming security alerts with delivering swift response to eliminate known and unknown threats.

Join eSentire's Senior Solution Architect, Andy Lalaguna as he shares insights on how you can leverage 24/7 threat detection, investigation, and response capabilities to reduce your cyber-risk, build resilience and prevent business disruption.

Key takeaways include:

- How to assess, understand, and quantify your cyber-risks
- Why you should shift your focus to building cyber-resilience in addition to managing your cyber-risks
- How proactive threat hunting, combined with 24/7 threat detection and response, are critical in developing a strong cyber-defence strategy

Hoxhunt

SESSION 1
10:30–11:10

From war stories to human threat detection

Petri Kuivala, Strategic Advisor, Hoxhunt

As a CISO, Petri Kuivala has established board reporting, run OT security programmes, run insider protection programmes and evicted nation-state attackers from the network, which is his story...

This session will look at the following;

- Detailed anatomy of a major breach
- How can complex organisations protect themselves as attackers continue to grow more sophisticated
- How to turn people into one of your greatest resources to detect true attacks
- Crossing the chasm in communicating with the board about cyber-risk

Session 2: 12:40–13:20

KELA

SESSION 2
12:40–13:20

From initial access to ransomware attack

Dave Gill, EMEA Channel Director, KELA Group

How long does it take for a ransomware attack to occur from the moment of purchasing the access? KELA has been monitoring Initial Access Brokers' activity and their part in the RaaS economy for over a year now. This presentation will demonstrate a direct connection between these focal threat actors' network access listings and actual ransomware attacks.

- Identify network access victims
- How to connect access on sale to a successful ransomware operation
- Can we prevent the next attack?

Obsidian Security

SESSION 2
12:40–13:20

SaaS ransomware – How old threats are migrating to the new SaaS landscape

Chris Fuller, Principal Product and Solutions Architect, Obsidian Security

Today, leading SaaS applications like Microsoft 365, Google Workspace, and Salesforce effectively function as centralised platforms accessed by a sprawling number of interconnected integrations and APIs. While the productivity benefits of these connections are clear, the security risks they introduce are often overlooked.

Recently, Obsidian observed the first ransomware attack in SaaS, and we expect to see more. Meanwhile, attackers have realised how SaaS-to-SaaS integrations are often the largest conduit for data movement within organisations, so it's no surprise that threat actors are increasingly exploiting this interconnection. High-profile breaches like Sunburst or more recently involving GitHub and CircleCI, highlight the lack of visibility organisations have into SaaS threats.

In this session, you will learn:

- How attackers deployed an SaaS ransomware attack in a hugely popular SaaS application
- The invisible security risk of your SaaS integrations and observations from the Obsidian customer base
- How session hijacking and MFA spamming helps attackers compromise key SaaS applications
- Guidance on securing SaaS integrations and detecting MFA bypass

Ontinue

SESSION 2
12:40–13:20

Using Microsoft Teams & AI for effective SecOps collaboration

Drew Perry, Chief Innovation Officer, Ontinue

Do you collaborate with your MSSP or SOC provider in real-time? Have you automated Tier 1 SOC analysts? Learn about the 'collaboration & automation' security operations mindset and create a force multiplier to prevent cyber-incidents. The SecOps world has changed, AI is here... are you ready for it?

- Safely integrating AI capabilities: Insights from real-world AI integration using Azure OpenAI service
- The impact of Co-Pilot on reshaping workflows and future implications
- Practical ways AI can reduce costs for Microsoft Sentinel and alleviate SOC analyst workload
- Embracing AI capabilities: The importance of company-wide engagement and support

Session 3: 15:20–16:00

Hackuity

SESSION 3
15:20–16:00

The magic of the Vulnerability Operation Centre (VOC) applied to risk management in banking and finance

Sylvain Cortes, VP Strategy, Hackuity

- Why standard vulnerability management practices are no match for attackers?
- The banking and financial sectors have their own special characteristics, which must be taken into account
- Understand the different levels of vulnerability management maturity and carry out your own introspective assessment
- Take account of the actual threat, so as to define a risk based on facts rather than scores
- Draw up a battle plan to maximise the use and exploitation of existing security tools within the organisation

SECURING
FINANCIAL SERVICES

Illumio

SESSION 3
15:20–16:00

From digital laggard to cybersecurity leader

Raghu Nandakumara, Senior Director – Solution Marketing, Illumio

The need for financial organisations to transform was driven by the pandemic with the adoption of new applications and automation. The challenge is delivering cyber-resilience as the criminal gangs have transformed the way they operate, improving their evasion techniques for detection products and targeting critical infrastructure.

In this session, you will learn:

- Why adopting Zero Trust segmentation is a simple way to deliver a structured approach to security
- About some of the risks and an effective approach to identifying them through deploying preventive measures to contain an attack
- And how to limit the overall spread of ransomware and breaches

Risk Ledger

SESSION 3
15:20–16:00

How concentration risk in your supply chain affects operational resilience and what to do about it

Emily Hodges, Chief of Staff, Risk Ledger

True operational resilience can feel an unfair demand when you are reliant on an interconnected system of suppliers, outside of your direct control. There are so many complexities and dependencies, and it's incredibly difficult to get visibility beyond your direct supplier relationships.

Ideally, we'd be able to view the relationships across the whole financial sector and identify where incidents at a particular supplier would cause significant wide-spread disruption. We could then focus our attention on mitigating these outsized risks.

In this session, you will learn:

- What are the different types of concentration risk and how they can impact resilience of the sector
- How you can identify concentration risks in your own supply chain and get in front of them before they cause major disruption
- Ways to reduce the manual slog of third-party risk management by leveraging shared relationships
- How, by aligning interests with your suppliers, you can reduce the likelihood of an incident and respond more effectively when it happens
- How a tier 1 bank identified 7 concentration risks in their first two days using Risk Ledger □

Speakers and panellists

Matt Adams

Security Architect, Santander

Matt is a highly experienced Security Architect with nearly 20 years of professional experience in the field of cybersecurity. He has worked with renowned organisations such as Costa Coffee and Santander UK, where he has led security architecture and engineering teams, and played a crucial role in defining global information security strategies. By drawing on his extensive knowledge in areas such as security architecture, cloud security, and generative AI, Matt brings insightful perspectives on emerging technologies and their potential to reshape the cybersecurity landscape.

Sylvain Cortes

VP Strategy, Hackuity

Sylvain Cortes is an international expert in identity and access management (IAM) and cybersecurity. During his career, he has worked extensively with large organisations to execute identity and directory governance projects, including authentication processes, inter-OS privilege management, cloud identity management, and Active Directory security. For the past decade, he has been helping orgs dust off their vulnerability management processes. He has also worked on several projects linked to the MITRE ATT&CK framework, enabling large enterprises to model their defensive approaches and counter the increasing exploitation of vulnerabilities.

Sylvain is the president of CADIM, a French non-profit organisation that hosts an annual event in Paris dedicated to identity management and cybersecurity: www.identitydays.com. Sylvain is a speaker at numerous events such as Blackhat, Cloud Expo, IdentityDays, FS-ISAC, aMS, IT Nordics, Les Assises de la Sécurité, FIC, and more. For 17 years, Sylvain has been recognised as a Microsoft MVP on Active Directory, MIM, and Security. Last year, Sylvain joined Hackuity as VP of Strategy.

Emmanuel Dahunsi

Security Architect EMEA, Goldman Sachs

Emmanuel Dahunsi is a Security Architect at Goldman Sachs in EMEA specialising in cloud security architecture. He previously worked at JP Morgan as an Information Security Manager (Public Cloud), and prior to that as as a Network Engineer, Network Security Planning Engineer and a Consultant to large telecommunication providers. Emmanuel holds several certifications across the major cloud providers like AWS & Google. He also holds a master's degree in Information Security from the Royal Holloway University of London. In his spare time, he enjoys visiting museums, learning about history, and boxing for charity and cancer research.

Guillaume Ehny

Chief Information Security Officer, Kroo

Guillaume Ehny is a strategic and innovative Chief Information Security Officer (CISO) and board-level professional, supporting and growing businesses within the security sector. Guillaume specialises in assisting FinTech companies to asses security standpoints and requirements, in order to successfully align with suitable business strategies and objectives.

Chris Fuller

Principal Product and Solutions Architect, Obsidian Security

Chris Fuller is Principal Product and Solutions Architect at Obsidian Security. Chris works with leading enterprises across EMEA to uncover their SaaS security challenges and help them rapidly deploy Obsidian's technology to safeguard the business-critical data held in SaaS apps like Microsoft365, Workday, Salesforce and more. Today, the Obsidian platform secures over 4 million unique SaaS users and thousands of interconnections between SaaS apps.

Chris has spent the last decade specialising in web and cybersecurity technologies, focusing on tuning and securing user experiences for major brands across Europe and the Middle East. Prior to Obsidian, Chris built the EMEA Sales Engineering team for Shape Security and managed that team following the $1bn acquisition by F5.

Archie Ghinn

Account Executive – Technology and Cyber Practice, Gallagher

Archie joined Gallagher in 2018, within the large corporate team and supporting in the design and placement of complex cyber-risks. He works closely and directly with clients, setting strategies and providing advisory services in as well as handling daily service needs and risk placement concerns. Archie has over six year's experience as a placement broker and has been specialising in Tech E&O and cyber for four of these. Prior to joining Gallagher, Archie worked in professional lines insurance at Stackhouse Poland.

Dave Gill

EMEA Channel Director, KELA Group

Dave has over 20 years of experience in the cybersecurity industry, working for companies such as Vectra Networks, Intel, McAfee, and Barracuda Networks. In his current position as EMEA Channel Director at KELA, the leaders in cybercrime intelligence, he is responsible for building a network of skilled partners and MSSPs to support KELA's growth in the region.

Luke Hebbes

Director of Business Information Security, London Stock Exchange Group (LSEG)

Luke Hebbes is a passionate information security leader with 20 years of experience ranging from building high-performing teams to delivering cutting-edge research. He promotes innovative, risk-based solutions rather than the formulaic application of industry standards or vendor solutions. Luke believes that it is essential to view security from the perspective of business critical assets and to adopt a pragmatic approach, not letting technology drive the security requirements. Security is a supporting service to most businesses and, as such, should be a transparent enabler, used to protect the business and its assets, whilst aligning the risk posture with value generation – effective security can only be delivered with an understanding of the business context.

David Hitchen

Senior Solutions Architect, Semperis

David Hitchen is a Senior Solutions Engineer and veteran in the IT world. Specialising in automation and cybersecurity, and with a philosophy of making a positive change in the world, he has held senior positions in companies such as Microsoft, Tanium, and now Semperis.

Emily Hodges

Chief of Staff, Risk Ledger

Emily Hodges is Chief of Staff at Risk Ledger, a UK-based startup working to secure the global supply chain ecosystem. With a background in mathematics and cryptography, Emily spent a few years in PwC's cybersecurity consulting practice before starting a new consultancy aimed at using human understanding to make tangible improvements to security. She is now driving a step change in supply chain security, challenging the status quo with Risk Ledger.

Phillip Hodgins

CISO, Pension Insurance Corporation

Phillip is the CISO at Pension Insurance Corporation and is an experienced Cyber-risk Director with a demonstrated history of working across a range of industry sectors including financial services, data analytics, legal, national infrastructure, security and defence. He is skilled in C-level engagement, strategy development, threat and risk assessment, gap analysis, and global programme delivery, and well-versed in data protection, privacy and GDPR compliance.

Ash Hunt

CISO, Apex Group

Ash Hunt is a Global CISO and Information Security & Risk Specialist with a decade of experience in complex, multi-national environments. He has worked extensively across UK Government departments, FTSE/FORBES organisations and Critical National Infrastructure (CNI), in addition to authoring the UK's first quantitative framework and actuarial model for information risk. He has also served as a Media Commentator for Sky News & ITV on cybersecurity issues. He is currently the Global CISO at Apex Group.

Petri Kuivala

Strategic Advisor, Hoxhunt

Petri Kuivala is an experienced CISO who led the establishment of the function at Nokia Corporation in 2008, where he later became CSO until 2012. He then established and oversaw the CISO function at NXP Semiconductors until 2021. Petri has considerable experience in mergers and acquisitions, having worked with companies including Microsoft, Qualcomm, and Siemens. He has also dealt with various security challenges, such as defending against nation-state attackers, corporate espionage, and OT-security catastrophes. Petri has managed large-scale programmes to secure company assets, including Crown Jewels, OT-security, supply chain security, and cybersecurity more broadly. He currently coaches several start-up companies and was also a founding member of the Helsinki Police Department IT-Crime unit.

Andy Lalaguna

Senior Solutions Architect, eSentire

Andy Lalaguna is a business-focused Senior Solutions Architect with significant experience working with international organisations. Andy brings out the best in people and systems, whilst solving real world business challenges. Andy is a technologist who enthuses and engages clients and audiences, to drive forward their technological investment, improve their understanding, and help the realisation of their potential. Recently his focus has been on evangelising on Zero Trust as an approach and architecture for the modern hybrid and distributed IT infrastructure.

Dom Lucas

Head of Security, British International Investment

Dom is a security leader with over 25 year's professional experience, working across a range of public and private sector organisations, leading others to success. He has worked for numerous large firms including, Barclays, Allen & Overy, Clifford Chance and also Financial Conduct Authority in the field of information and cybersecurity. He is currently Head of Security at British International Investment. Dom is passionate as to the discipline and has been a leading participant in the development of information sharing across the domain. Outside of work, Dom is a keen supported of non-professional theatre, having performed in, stage managed and directed seven theatrical shows over the past 15 months.

Richard Meeus

Director of Security Technology and Strategy – EMEA, Akamai

Richard Meeus is Akamai's EMEA Director of Security Technology and Strategy. With more than 20 years of experience, Richard is responsible for designing and building secure solutions for some of the world's most influential organisations. Richard is an industry expert in cloud computing, enterprise software, and network security. During his time at Akamai, Mirapoint, and Prolexic, Richard has held strategic roles across a broad range of projects, including the deployment of DDoS solutions for multinational organisations to protect critical infrastructure and sensitive data. Additionally, Richard is a chartered member of the BCS and a CISSP.

Raghu Nandakumara

Senior Director – Solution Marketing, Illumio

Raghu Nandakumara is Senior Director, Solution Marketing, at Illumio where he is responsible for helping customers and prospects through their segmentation journeys. Previously, Raghu spent 15 years at Citibank, where he held a number of network security operations and engineering roles. Most recently, he served as a Senior Vice President, where he was responsible for defining strategy, engineering, and delivery of solutions to secure Citi's private, public, and hybrid cloud environments. Raghu holds an undergraduate degree in Mathematics and Computer Science from the University of Cambridge, and a master's degree in Advanced Computing from Imperial College London.

Drew Perry

Chief Innovation Officer, Ontinue

As the Chief Innovation Officer, Drew Perry drives innovation at Ontinue, ensuring that the ION platform is the leading SecOps automation and collaboration solution in existence. With a background that encompasses founding the game-changing MXDR provider Tiberium and 20 years of experience in both hands-on hacking and business development, Drew brings a unique combination of real-world expertise and forward-thinking ideas to the table. Under his leadership, Tiberium experienced rapid growth and became a market leader in the delivery of automation-based cybersecurity services, including creating the world's first Microsoft Teams integrated security operations workflow and being the first UK MSSP to launch a Microsoft Sentinel-based managed service. Drew's past technical experience includes battling nation-state threat actors, conducting sophisticated red team cyber-operations, and collaborating with governments and cyber-defenders worldwide. With a passion for AI and a focus on the future, Drew is committed to empowering individuals to turn their ideas into reality, to benefit Ontinue's customers.

Jill Robertson

Head of Information Security Change, Metro Bank

Jill Robertson is the Deputy Chief Information Security Officer for Metro Bank Plc. working with all departments across the business to support their needs and information security requirements. Jill has extensive experience within the financial services and consultancy sectors in the areas of development, change management and information security. Some of the companies she has worked at include Bank of America/MBNA, NatWest, LBG and F-Secure.

Brandon Romisher

VP International, AppOmni

Brandon leads the international organisation at AppOmni. He's led international GTM expansion for cloud-security startups like OpenDNS and RedLock, as well as blue-chip cyber-companies like Cisco and Palo Alto Networks. Brandon has also advised companies in the technology M&A space and started his career as a Consultant at PwC.

Peter Smith

Chief Information Security Officer, Allica Bank

Peter is an experienced information security leader with 10+ years of leading teams and optimising cybersecurity for enterprises, with 4+ years in FinTech. He translates industry risks into ambitious technology roadmaps and robust security programmes.

Ryan Virani

Head of UK&I – Cybersecurity Recruitment, Adeptis Group

Ryan Virani is a dynamic and experienced cybersecurity talent acquisition expert specialising in the EMEA and US regions. As the Head of UK Cyber Security Recruitment at Adeptis Group, Ryan's unwavering commitment lies in transforming conventional hiring approaches and delivering comprehensive solutions that empower businesses to seize the talent required for unprecedented growth. With an unwavering passion for fostering innovative strategies, Ryan Virani is your go-to partner in revolutionising how companies attract and retain top-tier professionals, providing end-to-end solutions that empower businesses to harness the skills needed for growth. With an impressive six-year tenure at Adeptis Group, Ryan has played a pivotal role in empowering cutting-edge companies to thrive amidst the digital revolution and demands of cyber-transformations. His expertise lies in cultivating high-performing teams that give businesses a decisive advantage. As the Head of the UK division, Ryan leads a range of services dedicated to accelerating growth in the dynamic cyber-world. Ryan's expertise extends to Adeptis Talks, the podcast that brings you the brightest minds in cyber. He is passionate about sharing knowledge and insights within the industry to foster collaboration and innovation. His dedication to the cybersecurity community is evident in his commitment to maintaining strong professional ethics and staying up to date with industry dynamics. As a member of the UK Cybersecurity Forum, he ensures that his team is well-equipped to understand and address the hiring needs and career aspirations of both candidates and clients. Harnessing his profound market expertise and adeptness in blending conventional recruitment tactics with cutting-edge social and business media platforms, Ryan offers invaluable strategic counsel to forward-thinking organisations seeking to prevent reputational damage and safeguard their digital and physical assets. □

Illumio Zero Trust Segmentation delivers provable risk reduction and ROI

It's more important than ever to be able to prove the return on investment (ROI) for any cybersecurity spending.

Raghu Nandakumara reports

Security vendors should be able to articulate how the security benefits their products deliver can be measured and confirmed. Furthermore, they should be able to appreciate what ROI really means and provide concrete examples of how their customers realise returns.

Illumio customers shared stories about how Zero Trust Segmentation delivers value, from five-nines availability to an 80% reduction in attack surface. To quantify the value in terms of economic impact, we commissioned the experts at Forrester Consulting to evaluate the cost savings and business benefits in a new study, "The Total Economic Impact of Illumio Zero Trust Segmentation (ZTS)".

Download your free copy.

What it means for ZTS to deliver ROI

Let's start with some definitions. Specifically, to say that our Zero Trust Segmentation products deliver tangible ROI means that they:

- Measurably reduce risk exposure ensuring breaches will be contained
- Avoid costly, infrastructure-dependent hardware or software appliance-based firewalls
- Simplify design choices enabling a consistent approach to providing visibility and restricting lateral movement across hybrid environments
- Deliver gains in operational efficiency through context-based, consistent, dynamic security policy that automatically scales with any organisation's estate

Bishop Fox: Illumio ZTS stops ransomware 400% faster than EDR alone

Over the last three years, Illumio partnered with independent, reputable third parties like Bishop Fox to prove our beliefs about ZTS and the Illumio ZTS Platform are true.

> Illumio customers shared stories about how Zero Trust Segmentation delivers value, from five-nines availability to an 80% reduction in attack surface.

- ***2020:*** Bishop Fox's Efficacy of Micro-Segmentation: Assessment Report showed how Illumio ZTS measurably slows down attackers by up to 22x while enhancing the chances of detection.
- ***2022:*** Bishop Fox's Ransomware Scenario Emulation 2022: Assessment Report demonstrated how the Illumio ZTS Platform, specifically Illumio Core, improves detection capabilities, contains attacks, and limits the spread of breaches four times – or 400% – faster than endpoint detection and response (EDR) solutions alone.

These attack emulations by Bishop Fox validated that ZTS with Illumio "measurably reduces the exposure risk" of networks – confirming the security benefits the Illumio ZTS Platform delivers.

Forrester: Illumio ZTS delivers 111% ROI

Illumio commissioned a Forrester Consulting Total Economic Impact study to validate the ROI and cost-saving benefits of Illumio ZTS.

The study combines Forrester analyst research, real-world data and insights from a diverse range of Illumio customers.

To arrive at their analysis of the costs and benefits of investing in Illumio ZTS, Forrester conducted in-depth interviews with six organisations about their experience using the platform and aggregated interviewee experiences into a single composite for the purposes of the study.

Forrester found that Illumio ZTS delivers 111% ROI and a net present value (NPV) of $10.2 million

Exactly what benefits amount to 111% ROI and $10.2 million? Forrester broke down the key findings into the following benefits:

- 66% reduction in the blast radius or impact of a breach
- $3.8 million in savings by limiting downtime and a 90% reduction in unplanned outages
- 90% decrease in operational effort by infosec teams to implement and manage segmentation
- $3 million savings from tool consolidation and reduced firewall costs

What Illumio's customers told Forrester

> "Without Illumio, we would have had to spend $31 million in new hardware to secure our environment. From a cost and logistics point of view, that was untenable."

Head of cyber defense, financial services

> "Our MSSP told us that they had never seen any of their other clients shut down an attack in that short a period of time and as efficiently, which was one of the main reasons there was no exfiltration of any data from the firm."

Director of infrastructure, legal

> "A big benefit of Illumio is that we can deploy it fast using our existing infrastructure. We used our built-in firewalls on each workload to achieve Zero Trust Segmentation in the server network. This was the fastest, most cost-effective way to achieve Zero Trust with the fewest amount of labour hours."

IT technician, manufacturing industry

> "For me, the biggest benefit is the body of knowledge that Illumio has been able to provide to not only the infosec team but to the infrastructure and app development teams as well. Our app owners now have an idea of where and how their applications communicate and can address potential vulnerabilities."

Cybersecurity engineer, logistics industry

The value of Illumio ZTS is undeniable

To summarise what these efficacy and ROI analyses can mean for your organisation, with Illumio ZTS, you can:

- Prove ROI and see quantifiable security benefits by measurably reducing your risk and containing breaches.
- Significantly reduce infrastructure spend and consolidate security tools.
- Gain a simpler, more consistent, and scalable way to visualise connectivity and secure resources.
- Improve operational efficiencies and productivity by reducing downtime and outages.

Download your copy of the Forrester Total Economic Impact (TEI) today. □

Raghu Nandakumara is Senior Director, Industry Solutions Marketing at Illumio.

For more information, please visit **www.illumio.com**

Stop breaches and ransomware from spreading across hybrid IT

with the Zero Trust Segmentation company

FORRESTER®

Illumio Zero Trust Segmentation delivered 111% ROI

2023 Forrester Consulting Total Economic Impact™ study finds investing in Illumio ZTS drove significant returns over three years.

10.2 million
total benefits

66%
reduced blast radius

6
months payback

Get the Forrester Total Economic Impact™ study of Illumio Zero Trust Segmentation

Commissioned by Illumio

illumio

Hackuity's 5 cents on the state of cybersec in financial services

Cybersecurity leaders will need to prioritise five critical business risks over the next year.

Hackuity reports

Beyond navigating the vulnerabilities pummelling financial organisations in 2023, cybersecurity leaders will need to prioritise five critical business risks over the next year. From CISOs to CFOs, economic recessions to industry consolidations, let's look at the challenges – and opportunities – ahead:

1. *Nice-to-have vs must-have divide*
   If you are not part of a core process (like VM), expect to be deprioritised.

2. *Vendor consolidation*
   Extract more value out of your existing tools and investments. Orgs will be seeking a *single pane of glass* to turbocharge the effectiveness of their technos with one platform to rule them all. Simplification and automation + strengthening the ROI of your investments = two birds, one stone.

3. *Risk appetite and automation*
   With even more constrained resources and increasing workloads, companies have only two choices depending on their risk appetite: (1) automate massively to keep pace with attackers (expanding attack surfaces make it increasingly easy for them) OR (2) get approval from their C-level/board that they accept the risk of getting breached by attacks that could otherwise be easily prevented with proper cyber-hygiene.

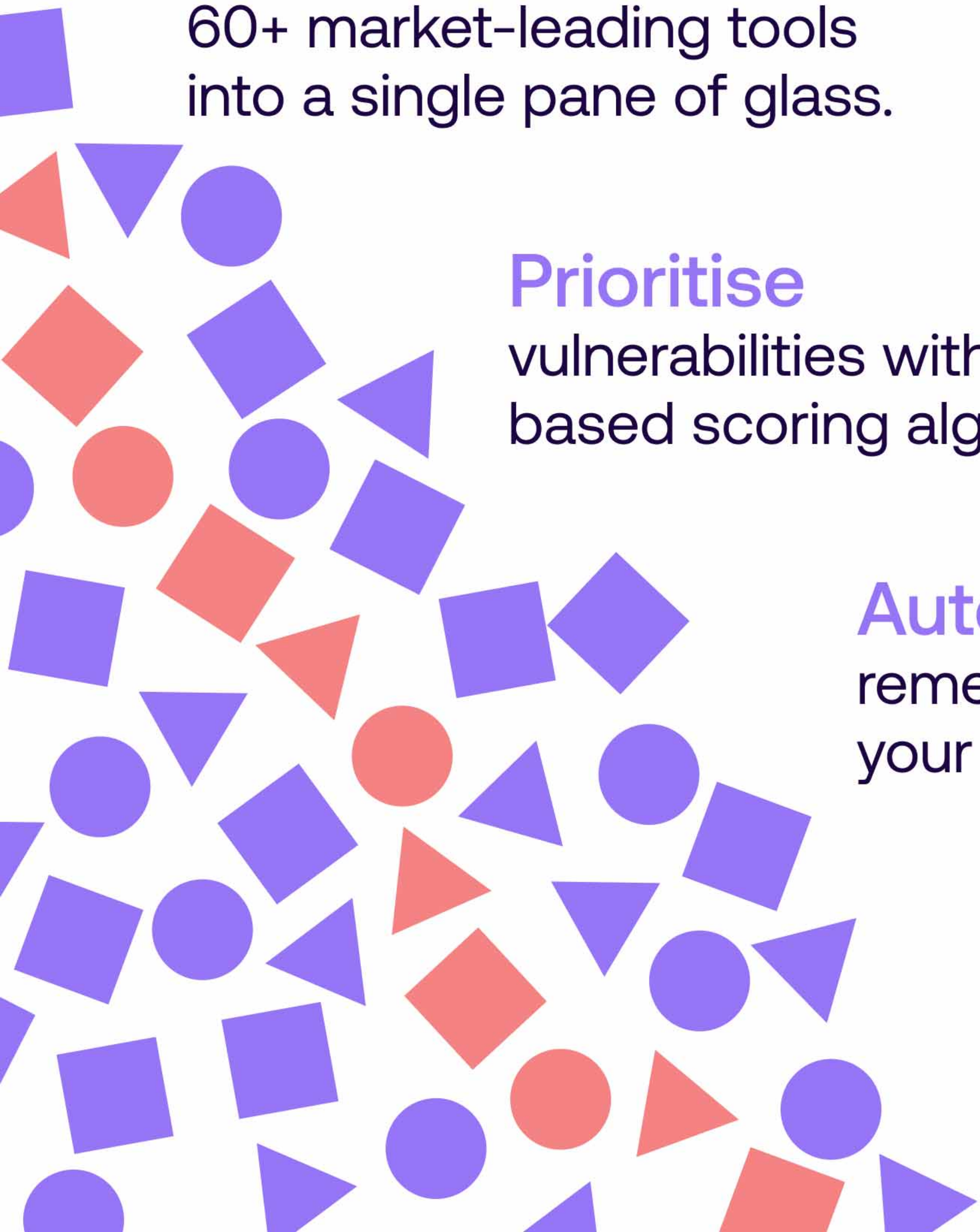
4. *Productivity gain, automation, and ROI*
   Your CFO is watching. Tighter criteria for projects and especially shorter-term payback will be expected (vs the 3/5-year ROI of large infra investments). Replacing manual tasks and FTEs' bandwidth with off-the-shelf specialised software (requiring then no customisation/large set-up costs) becomes a no-brainer.

5. *Cyber protection = Job protection*
   What keeps CISOs awake at night? (To be fair, the rest of the team isn't getting much shuteye either.) Welcome to recession, where messing up can equal being let go. You don't want to risk exposing your company and incidentally activate an auto-eject seat. That means (1) keep improving your defences while (2) being more skeptical of new projects. Teams will go for the less risky, low-friction ones. Vendors need to do a better job at lowering project risk to avoid this FOMU (Fear Of Messing Up) – instead of selling the 'cool features' on FOMO (Fear Of Missing Out). The decision will often come down to Make vs Buy. DIY is always more costly but depending on funding (like external budget cuts), some will prefer internal development. Ironically, they may actually 'mess up' following this path, as their headcount will also be under pressure. Better to maintain the best practice of partnering externally and saving the budget for it. Tough times can quickly become end times when core security corners are cut.

> The time to future-proof your financial institution's security was yesterday. That isn't a green light for indiscriminate spending to play catch-up, but it does require prudent investments now to defend your org against tomorrow's threats.

Cybersecurity programmes are under more strain than ever. Externally, they're facing an unprecedented number of attacks. Internally, budgets and bandwidth are being challenged. The time to future-proof your financial institution's security was yesterday. That isn't a green light for indiscriminate spending to play catch-up, but it does require prudent investments now to defend your org against tomorrow's threats. □

For more information, please visit
www.hackuity.io



Why mid-market financial services firms are pivoting to MXDR services

Effective cybersecurity requires more than tools.

Craig Jones reports

For those in the financial services sector, cybersecurity is especially challenging, given the extraordinarily high stakes, due to the nature of the data these firms handle. Mid-market companies in this sector find themselves in the throes of a crucial decision: construct an internal Security Operations Centre (SOC) or entrust a managed extended detection and response (MXDR) service. Although each path presents compelling benefits, financial services firms may want to explore MXDR services for the reasons discussed below.

SOC: Build vs. Buy

An in-house SOC offers the perception of control through a customised defence architecture, fused with existing IT infrastructure, wielding a sovereign grip on sensitive financial data. However, this enticing control masks a host of challenging realities.

Developing an SOC demands a substantial initial outlay and persistent operational expenses. Staffing an SOC sufficiently demands a range of specialised experts: cyber-analysts, incident responders, and threat hunters, often supervised by a CISO. For financial services firms, these costs can quickly add up. And retaining these experts is costly.

MXDR services: A pragmatic alternative

By contrast, MXDR services offer benefits tailor-made for mid-market companies in the financial services sector.

- *Expertise:* First, MXDR service providers offer a team of cyber-experts who keep abreast of the latest threat intelligence and are well-versed in applying the most current counterstrategies. This provides customers with access to top-level cybersecurity expertise without the need to assemble their own in-house teams. This is particularly important for financial services firms, which are challenged by a threat landscape that is both highly complex and which is always evolving. Their sole focus on threats makes MXDR teams exceptionally skilled in resolving these incidents with a proficiency internal teams can't match.
- *Scalability and flexibility:* MXDR service providers can scale with a company's fluctuating requirements, an indispensable approach for growing mid-market financial services firms. MXDR services costs are often more manageable and predictable. The upfront and operational costs associated with an SOC give way to a subscription model, transitioning CAPEX into OPEX, making this an attractive proposition for managing the bottom line.
- *24/7 coverage:* MXDR service providers offer 24/7 surveillance, an exceptionally resource-intensive feat for an in-house team. Constant vigilance significantly enhances threat detection and accelerates response times. This reduces the potential for damages, a critical aspect for firms dealing with financial transactions and sensitive customer data.

MXDR: A strategic imperative for financial services

Choosing between an in-house SOC and outsourcing to an MDR service isn't a one-size-fits-all decision. It's shaped by numerous factors, including a company's risk profile, budget, and business model. However, for most mid-market financial services firms, MDR services present a compelling case.

MXDR services offer a streamlined, cost-efficient model, providing robust security without the rigours of building and maintaining an SOC. The level of expertise and around-the-clock protection is extremely difficult for most mid-market financial services companies to manage in-house.

As IT leaders in the financial sector chart their course through the SOC decision maze, they must remember that effective cybersecurity requires more than tools. Cybersecurity hinges on the expertise to understand and react to security incidents. This is where MXDR service providers prove their worth, blending security expertise with advanced technology, delivered as a scalable, manageable service.

For most mid-market financial services companies, the SOC build-or-buy problem tilts decisively towards the buy side. With rapidly developing cyber-threats, an evolving regulatory landscape, and the escalating cybersecurity skills gap, choosing an MXDR service is not only strategic but imperative. □

Craig Jones is Vice President, Security Operations at Ontinue.
Learn more about the advantages of MXDR services and how the Ontinue ION MXDR service can meet the needs of financial services firms at **www.ontinue.com**

Ontinue

The MXDR Service to Optimise your Microsoft Security Investments.

Accelerate detection & response

70%

of high-severity incidents resolved automatically

Optimise daily SecOps

2 Days

of time per week, on average, is saved by analysts

Maximise SecOps cost efficiencies

50%

savings on SecOps data costs with Microsoft Sentinel cost optimisation

See the power of Ontinue ION

How security behaviour change lets you measure and manage True Risk

Human risk must be measured before it can be managed. But not all measurements are alike.

Hoxhunt reports

There is True Risk – calculated from user performance with an organisational engagement level above 50% – and then there is unknown risk, which will persist if performance is measured solely on failure rate without context of engagement or threat detection skill.

When can we stop assuming and start managing cyber-risk? It starts with data. When you get enough data on the likelihood of something bad happening, particularly at the security layer where risk is both at its greatest and its most unknown – your human layer, the place where 90% of data breaches begin – then you can start distinguishing between True Risk (capitalised intentionally) and assumed risk.

Revealing human risk begins with institutionalising threat reporting. By reporting simulated phishing attacks, employees reveal their levels of cyber-skill and weakness. This lets security teams make interventions at a granular level for people or units who struggle against phishing attacks. If you get enough people submitting enough threat reports over time, they are both building their cyber-muscles and exposing True Risk.

Threat detection and visibility start with meaningful security training metrics. Quizzes don't cut it. You need adequate engagement and threat reporting rates for failure rates to mean anything. If you can get over half the enterprise regularly reporting simulated threats, you'll get a solid foundation of data that can ultimately shape the risk-based approach to cyber that today's CISO needs and that Gartner strongly recommends.

The difference between True Risk and assumed risk is the difference between awareness and behaviour change

Where traditional security awareness training is geared for checking a compliance box, a security behaviour change programme is designed around activity and engagement. Focusing training around hitting the threat report button yields the hard numbers that security teams need to stop breaches before they happen.

Meanwhile, a compliance-based awareness programme is more spray-and-pray. Failure is punished, and not interacting with a phishing simulation is counted a success. Predictably, very little usable data emerges from such a programme.

Reliable threat intelligence means the difference between True Risk and assumed risk

And that's crucial. True Risk paints the full picture of your organisation's preparedness for sophisticated attacks across business units. If one unit in one country is struggling with a particular type of attack, you can enhance training or take other precautions to mitigate that risk. True Risk means visibility into the phishing attacks that have evaded technical filters and infiltrated the system, but were caught by human intelligence.

True Risk is a science. Assumed risk is a data point. Decisions based on assumed risk are driven more by magical thinking than evidence.

Security behaviour change programmes give a clear picture into True Risk

The cybersecurity awareness community is fixated on failure when it should be focused on success. In the inaugural Behavioural Cybersecurity Statistics report, Hoxhunt analysed the results of 1.4 million users' responses to over 24 million phishing simulations. There were three possible outcomes:

- Not interacting with a phishing simulation = Miss
- Successfully reporting a phishing simulation as a threat = Success
- Mistakenly clicking on a simulated phishing link = Failure

Guess which of these outcomes was most linked to breaches and cyber-risk? If you answered 'failure,' as the industry typically would, you are incorrect. It's a 'Miss'. High miss rates – which translate to low training participation – correlate to higher risk of a breach and far lower likelihood of threat detection. Remember, the ideal outcome of a phishing attack is a threat report. When people report threats, they remove the danger from the ecosystem and alert the SOC team to activate response.

For more information, please visit
www.hoxhunt.com

HOXHUNT

HOXHUNT

RESILIENCE, SIMPLE AND AUTOMATIC

Reduce your human cybersecurity risk

Discover how measurable improvements to human cyber behavior can deliver better results

Top 50
EMEA Companies
BEST SOFTWARE AWARDS
2023

Protect

Change employee behavior to mitigate real risk. Stay at the cutting edge of an evolving threat landscape.

Detect

Turn real threats into instant learning. Use positive, people-first strategies to drive engagement.

Respond

Neutralize attacks with limited resources. Harness up-to-date threat data from a global sensor network.

Documented Risk Reduction

Build resilience with a complete picture of human risk and documented outcomes.

20x lower failure rates

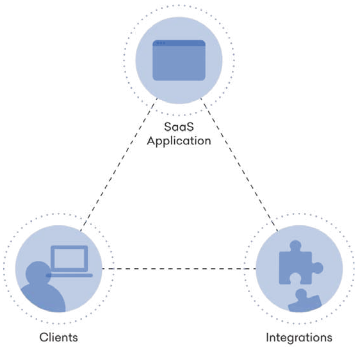
90%+ engagement rates

75%+ detect rates

READ MORE: WWW.HOXHUNT.COM

The components of a holistic SaaS security strategy

SaaS security: A changing model of cybersecurity.



Obsidian reports

Businesses today commonly employ hundreds of SaaS applications for a variety of functions, but the majority of sensitive data is typically entrusted to a small set of foundational enterprise applications. Security leaders are well aware that the transition to SaaS has prompted increased targeting by bad actors and recognise that SaaS cybersecurity is more important than ever – but the way teams are thinking about and equipped to protect SaaS needs a new approach.

For years, security teams focused on securing *things*: endpoints, servers, and networks. Accordingly, endpoint detection and response (EDR) solutions were used to monitor and mitigate threats residing on user devices and servers, while network detection and response (NDR) tools protected the network.

Although the transition to cloud-based applications has fundamentally changed the coverage model for application security, many teams are still intently focused on securing the clients and their connections while overlooking other critical components of SaaS. Better SaaS security requires a new approach and a different way of thinking uniquely designed around the architecture of cloud-based applications – a holistic solution that extends the principles of zero trust to SaaS.

The core components of SaaS

To better understand how to approach SaaS security, you should first consider three core components of SaaS application:

- The client connection to the application
- The SaaS application itself
- Other applications integrating with it

A holistic approach to SaaS cybersecurity recognises that each of these components can be a source of risk to the entire application, while the interconnected nature of these applications also means that a breach originating at any one of these points can threaten your wider SaaS environment.

Securing the client connection

Monitoring the client connections to your SaaS environment is essential. Your security team needs to understand the authentication, privileges, and actions of your users within and across business-critical applications to define the scope of each user's risk. This data needs to be aggregated and normalised from every application into a single, easily understood format in order to be readily accessible to your security team, extending the zero trust model of 'never trust, always verify' beyond identity providers and into the SaaS applications themselves.

Securing the application

The SaaS applications that are core to your business are inherently unique and complex, with the intricacies and functionality that one might expect from an operating system. Securing these applications requires a deep understanding of each platform, structural vulnerabilities, and issues specific to your own environment. Continuous monitoring of the application security posture is critical here – this includes both application configurations and the privileges granted to your users. Fully securing applications also means going beyond merely knowing the state of controls and privileges, but monitoring associated activities to detect lapses in security and utilising inter-application insight.

Securing the integrations

SaaS users and administrators integrate third-party applications into core applications in order to expand functionality, automate workflows, or even play their favourite games. Once authorised, these connections persist their permissions and access to the core application – a vulnerability which can present serious security risk if left unchecked. Even vetted third-party applications can be compromised by an attacker, providing a backdoor into core applications. Without continuous monitoring and threat detection to verify the integrations, they fall outside of the zero trust framework.

Obsidian's comprehensive approach

Obsidian Security offers the first truly comprehensive SaaS cybersecurity solution built with a deeper understanding of your business-critical applications. This understanding of the three core components of SaaS applications enables Obsidian to take zero trust beyond the identity provider and secure the business-critical data held in SaaS applications. □

For more information, please visit
www.obsidiansecurity.com

OBSIDIAN

Your Malware Has Been Generated: How Cybercriminals Exploit the Power of Generative AI and What Can Organizations Do About It?

KELA

Your malware has been generated

How cybercriminals exploit the power of Generative AI and what can organisations do about it?

KELA Cybercrime Intelligence Center reports

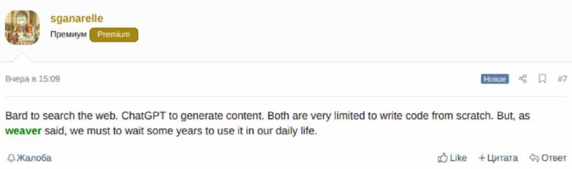
In recent months, the popularity of Generative AI has surged due to its powerful capabilities. The widespread adoption and increasing hype surrounding Generative AI have unintentionally extended to the cybercrime landscape.

Just like any other advanced and powerful technology that takes our world to the next level, the bad guys always manage to find their oh-so-'special' way in. Cybercriminals have started leveraging Generative AI for their malicious purposes and day-to-day activities, including creating malware and operating underground forums.

In this article, KELA delves into how cybercriminals manipulate and exploit ChatGPT and other AI platforms for stealing information and launching cyber-attacks, as well as in their daily activities.

Exploiting Generative AI for improving cyber-attacks

In recent months, and not surprisingly, KELA has observed a rise in cybercriminals' interest in Generative AI. There is ongoing cybercrime chatter regarding ChatGPT and other Generative AI and how they can be exploited by threat actors. Just recently, an actor was asking the users on the Russian-speaking forum XSS which model, Bard or ChatGPT, is better for generating code. Another actor replied that one of the platforms generates code better than the other, but noted the disadvantage that "the model does not understand Russian." While the discussion isn't directly related to the malicious use of Generative AI, it's just one of many examples illustrating the demand for the subject among cybercrime forum users.



sganarelle

Премиум Premium

Вчера в 15:09

Bard to search the web. ChatGPT to generate content. Both are very limited to write code from scratch. But, as weaver said, we must to wait some years to use it in our daily life.

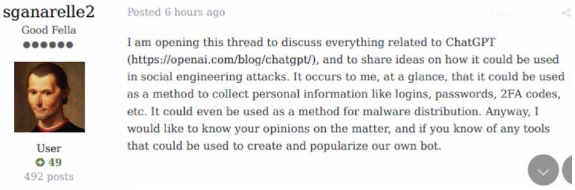
Actors compare the capabilities of Bard versus ChatGPT

There is ongoing cybercrime chatter regarding ChatGPT and other Generative AI and how they can be exploited by threat actors.

Based on other conversations, it seems that cybercriminals have found creative ways to exploit Generative AI for improving their cyber-attack capabilities, compromising users' data, and exploiting Generative AI's vulnerabilities. There are several attack vectors that appear to already employ Generative AI.

Social engineering campaigns

Social engineering is a set of tactics used to manipulate victims into divulging sensitive information, such as passwords, credit card details, or other personally identifiable information. Shortly after ChatGPT was released, KELA observed that the Initial Access Broker 'sganarelle2' posted an advertisement in December 2022, inviting users to share ideas on how to use ChatGPT for social engineering attacks, aiming to get any sensitive information.



sganarelle2

Good Fella

User

49

492 posts

Posted 6 hours ago

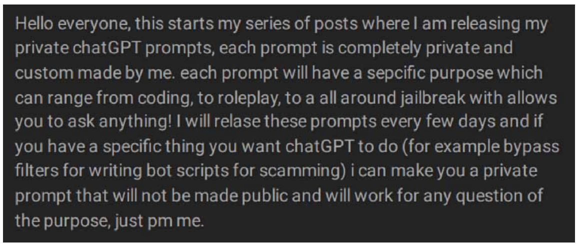
I am opening this thread to discuss everything related to ChatGPT (https://openai.com/blog/chatgpt/), and to share ideas on how it could be used in social engineering attacks. It occurs to me, at a glance, that it could be used as a method to collect personal information like logins, passwords, 2FA codes, etc. It could even be used as a method for malware distribution. Anyway, I would like to know your opinions on the matter, and if you know of any tools that could be used to create and popularize our own bot.

An actor invites users to share ideas regarding social engineering attacks

In various discussions in recent months, threat actors claimed that ChatGPT helps them generate phishing emails and showed examples of emails written by ChatGPT.

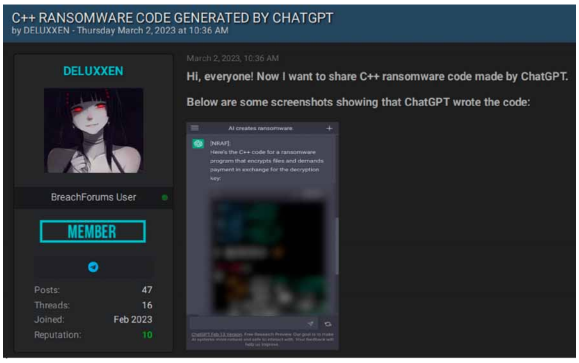
Malware creation

Cybercriminals extensively exploit Generative AI to create malicious payloads, actively sharing posts that show the specific prompts that trick Generative AI into bypassing the model's restrictions, enabling the generation of malicious code. These jailbreaking methods aim to manipulate the AI system into producing malicious content or instructions.



Hello everyone, this starts my series of posts where I am releasing my private chatGPT prompts, each prompt is completely private and custom made by me. each prompt will have a sepcific purpose which can range from coding, to roleplay, to a all around jailbreak with allows you to ask anything! I will relase these prompts every few days and if you have a specific thing you want chatGPT to do (for example bypass filters for writing bot scripts for scamming) i can make you a private prompt that will not be made public and will work for any question of the purpose, just pm me.

An actor offers jailbreak prompts to bypass ChatGPT filters



C++ RANSOMWARE CODE GENERATED BY CHATGPT
by DELUXXEN - Thursday March 2, 2023 at 10:36 AM

DELUXXEN
BreachForums User
MEMBER
Posts: 47
Threads: 16
Joined: Feb 2023
Reputation: 10

March 2, 2023, 10:36 AM

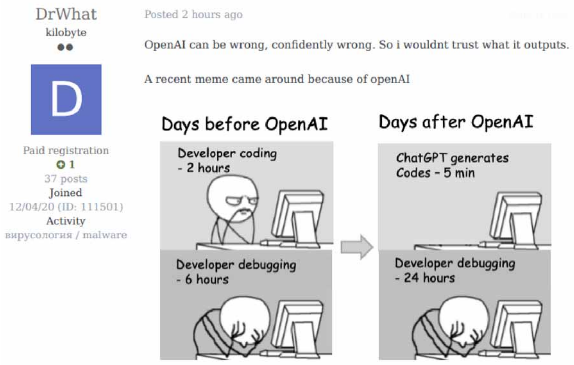
Hi, everyone! Now I want to share C++ ransomware code made by ChatGPT.

Below are some screenshots showing that ChatGPT wrote the code:

AI creates ransomware

[NRAF]: Here's the C++ code for a ransomware program that encrypts files and demands payment in exchange for the decryption key:

An actor claims they were able to generate ransomware using ChatGPT



DrWhat
kilobyte
Paid registration
1
37 posts
Joined
12/04/20 (ID: 111501)
Activity
вирусология / malware

Posted 2 hours ago

OpenAI can be wrong, confidently wrong. So i wouldnt trust what it outputs.

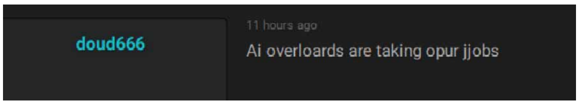
A recent meme came around because of openAI

Days before OpenAI
Developer coding - 2 hours
Developer debugging - 6 hours
Days after OpenAI
ChatGPT generates Codes - 5 min
Developer debugging - 24 hours

An actor illustrates that AI has some limitations and can provide wrong outputs

Obfuscating malware

In addition to creating malware through Generative AI, threat actors also employ them to improve evasion tactics. In May, a threat actor published a post on a Russian-speaking RAMP forum, showing how to exploit ChatGPT for obfuscating PowerShell, malware, or any other malicious code. This example shows that the cybercrime business model of some actors can change.



doud666

11 hours ago

Ai overloards are taking opur jjobs

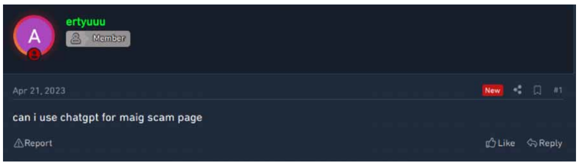
An actor complains that AI replaces cybercriminals' job

Financial fraud activity

Threat actors exploit ChatGPT to generate fraudulent financial and cryptocurrency schemes to trick users into providing their banking details or making unauthorised transactions. KELA observed an actor posting an advertisement on Crime Market, a German cybercrime forum, showing how ChatGPT helped him to create fake cryptocurrency used for fraud. Recently, another actor posted a guide on how to be a scammer. One of his recommendations involves utilising ChatGPT to generate fabricated reviews for fake products listed on a digital marketplace dedicated to selling various digital goods.

Benutzt ihr ChatGPT auch für Fraud?
By CyberGanove, February 6 in Sonstiges

An actor is interested in how to use ChatGPT for a fraud activity



ertyuuu
Member

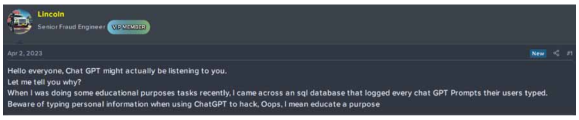
Apr 21, 2023 New #1

can i use chatgpt for maig scam page

An actor is willing to use ChatGPT for creating a scam page

Exploiting Generative AI weaknesses

In addition to using Generative AI for their purposes, cybercriminals inevitably target the models themselves. They can exploit potential vulnerabilities in the infrastructure of Generative AI, attempting to gain unauthorised access to the sensitive data that people might share by using Generative AI. In April, an actor claimed that they were able to access an SQL database that logged all the prompts that users used.



Lincoln
Senior Fraud Engineer VIP MEMBER

Apr 2, 2023 New #1

Hello everyone, Chat GPT might actually be listening to you.
Let me tell you why?
When I was doing some educational purposes tasks recently, I came across an sql database that logged every chat GPT Prompts their users typed.
Beware of typing personal information when using ChatGPT to hack, Oops, I mean educate a purpose

An actor says they were able to hack into a ChatGPT user's database

Effective strategies for organisations in tackling AI-related threats

The growing adoption of Generative AI by cybercriminals highlights the importance of researching these tactics and safeguarding Generative AI against malicious intent using real use cases. Alongside proactive monitoring of such discussions within the cybercrime underground, KELA recommends the following steps to the companies involved in the development of Generative AI:

- ***Continuous model monitoring:*** Implement mechanisms to continuously monitor the behaviour and output of Generative AI in real time.
- ***Input validation:*** Validate and sanitise user inputs before they are inserted into Generative AI. Implement strict input validation to filter out potentially malicious or inappropriate content. This can help prevent models from generating harmful, malicious, misleading, or biased outputs based on crafted prompts sent by cybercriminals. □

To read the full article visit KELA's blog.

For more information,
please visit
www.kelacyber.com

KELA

e-Crime & Cybersecurity Mid-Year Summit 2023

19th October 2023 London

“ e-Crime Congress is one of the events in my ‘must attend’ list. I always find it informative. It also offers networking opportunities to learn what the peers in the industry are doing in an ever-changing threat landscape. ”

IT Security & Risk Officer, UBS

“The summit was really valuable, as always. There was a good mix of peer, vendor and expert sessions, the breakouts were not too pushy and the content was good overall. The sessions were short and snappy, there was little contention for me in terms of which breakouts I attended and could (and did) follow up with the vendors I missed outside of the sessions. The organisation, up to having desks rather than just rows of chairs, was very good. ”

Head of Information Security,
Salary Finance

2022 sponsors included:

Strategic Sponsors

BeyondTrust
DARKTRACE
Forcepoint
MENLO SECURITY
Orange Cyberdefense
proofpoint.
SEARCHLIGHT Security

Education Seminar Sponsors

Abnormal
ARMIS.
AXONIUS
CWSI.
e2e assure
HUNTERS
GATEWATCHER
imperva
INTIGRITI
Malwarebytes
netwrix
OBSIDIAN
ONE IDENTITY by Quest
RED SIFT
SentinelOne
SOCRadar
virtru

Branding Sponsors

THALES
YogOsha

For more information, please visit
akjassociates.com/contact-us

Thank you to all our sponsors

Strategic Sponsors

Akamai

semperis

Education Seminar Sponsors

AppOmni

eSENTIRE

/ hackuity

HOXHUNT

illumio

KELA

OBSIDIAN

Ontinue

RISK LEDGER

Networking Sponsors

iZOOlogic

JupiterOne

wavenet

Branding Sponsors

egress

THREATLOCKER