SOLUTION BRIEF

Passing the (Pen) Test

Insights from network detection and response that enable financial services security operations and regulatory compliance

Financial services institutions (FSI) remain a top target for cybercriminals. In 2020 Financial and Insurance business had 721 incidents, 467 with confirmed data disclosure according to the 2021 Verizon Data Breach Investigation Report[1]. 56% of all attacks were from external actors primarily using credential attacks, phishing or ransomware.

The financial services sector is highly regulated, and governments rightly view their financial institutions and systems as part of their nation's critical national infrastructure (CNI). Additionally, legislative and compliance responsibilities around cybersecurity risk and posture fall on FSI—this includes building and testing organisational resilience.

Regulatory assessment tools such as CBEST in the UK, the European TIBER-EU, Federal Financial Institutions Examination Council (FFIEC) in the US and New York State Department of Financial Services (NYSDFS) cybersecurity regulations and frameworks take an intelligence-led approach to identifying salient threats to FSI organisations. They are required to demonstrate the use of independently delivered penetration testing and the ability to protect against identified risks.

> "Regulatory oversight is greater and greater, and we have to prove that a control is working. Cognito gives us transparency so we can find control weaknesses and remediate them quickly."
>
> **Deputy CISO, Leading Securities Exchange**

KEY HIGHLIGHTS

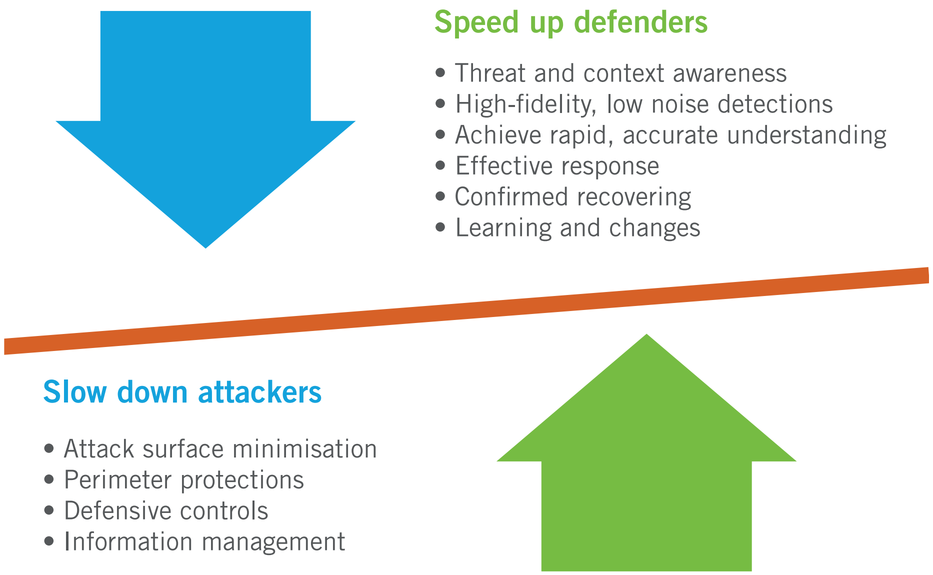
- The demarcation and areas of security responsibility between cloud service providers (CSP) and FSI must be clearly defined and covered through appropriate controls.
- By analysing anonymised metadata shared from hundreds of Cognito NDR platform deployments, Vectra has identified attacker behaviour insights that expose tactics that remain open to abuse.
- Vectra's AI powered Cognito NDR augments the defending "blue team" with high-fidelity attacker TTP behavioural detections which are prioritised by risk/certainty index™, profiled by attack type and the totality of the effected hosts and accounts are displayed as attack campaign.

[1] https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

Impede the bad, accelerate the good and prove your capabilities

Optimising FSI security posture can be considered in two dimensions— slowing down attackers whilst simultaneously speeding up the pace in which defenders are able to work. Identifying potential threats and placing appropriate protective controls are rational first steps but it is important to recognise that persistent, motivated and skilled attackers will always find a way inside an organisation's digital infrastructure.

It's impractical to implement security controls for every risk, or to train and test incident response (IR) teams against every threat the FSI faces, moreover the global threat landscape. Security leaders must balance these two dimensions within their organisation's unique operating context.



Speed up defenders

- Threat and context awareness
- High-fidelity, low noise detections
- Achieve rapid, accurate understanding
- Effective response
- Confirmed recovering
- Learning and changes

Slow down attackers

- Attack surface minimisation
- Perimeter protections
- Defensive controls
- Information management

Focus and prioritisation of key risks enables the provision of appropriate security controls and testing to enable your current security posture and IR capabilities are understood and of acceptable performance.

Advances in network detection and response (NDR) capabilities make it possible to provide automated, high-fidelity threat detection alerts while suppressing the noise of inaccurate detections or benign alerts. It also collects metadata from all network traffic —cloud, data centre, IT, and IoT — and enriches it with security insights and context. Aggregations of these insights provide industry sector and global intelligence on observed attacker behaviours. This can inform and increase the accuracy of the intelligence-led threat modelling exercises as part of the requirements of FSI cybersecurity penetration test planning.

Additionally, NDR's direct capabilities integrate into security operations' tools and processes. This enables FSI security teams to use high-fidelity threat detection alerts supported by a trail of forensic evidence for faster, more conclusive incident investigations to identify unannounced penetration tests, and proactively hunt for threats across the totality of the FSI digital enterprise.

> Advances in network detection and response (NDR) capabilities make it possible to provide automated, high-fidelity threat detection alerts while suppressing the noise of inaccurate detections or benign alerts.

Protect shared infrastructures, services, and your digital supply chains

FSI increasingly adopt cloud services and platforms for agility, scale and economic benefits. Cloud adoption can bring a concentration of risks through the consolidation of multiple services onto a single platform—making a rich target for would be attackers. A multi-cloud strategy can mitigate some of this risk but comes with additional complexity when attempting to build a cohesive security capability that spans on-prem, cloud and remote worker access. The demarcation and areas of security responsibility between cloud service providers (CSP) and FSI must be clearly defined and covered through appropriate controls. Regardless of the cloud operating model —SaaS, PaaS, IaaS, etc.— one constant is the requirement for the FSI to own identity controls.

> It is prudent to have proactive engaged CSPs and MSSP and external suppliers, prior to any penetration testing, understand responsibilities and responses during a security incident.

At the same time service providers and other suppliers create an extended attack surface and can fall into scope of a regulatory testing if they contribute to the delivery of FSI systems. As such it is prudent to have proactive engaged CSPs and MSSP and external suppliers, prior to any penetration testing, understand responsibilities and responses during a security incident. Consider including them in in-house tabletop incident response exercises to experience how they react and identify operating gaps.

Sunburst Supply Chain Attacks

Abuse of cloud infrastructure and a digital supply chain were brought into sharp focus in the Sunburst "Solarwinds" supply chain compromise that trojanised their update, infecting an estimated downstream 18,000 organisations.

The Washington Post reported that Russian group APT29 or "Cozy Bear" had breached the US Treasury and Commerce Departments as part of this compromise.

After initial penetration through the compromised SolarWinds application, they compromised the network further, using privileged accounts to move laterally and eventually obtain the credentials of a domain administrator account or the SAML Signing Certificate.

This allowed the attackers to move laterally to any on-premises device, or any cloud infrastructure.

This level of access could be leveraged to forge new privileged accounts and develop a sturdier foothold within an organisation.

As part of the techniques used to gain a foothold and further compromise, the attacker was observed performing Domain Federation trust activities.

Accelerate Incident Response maturity

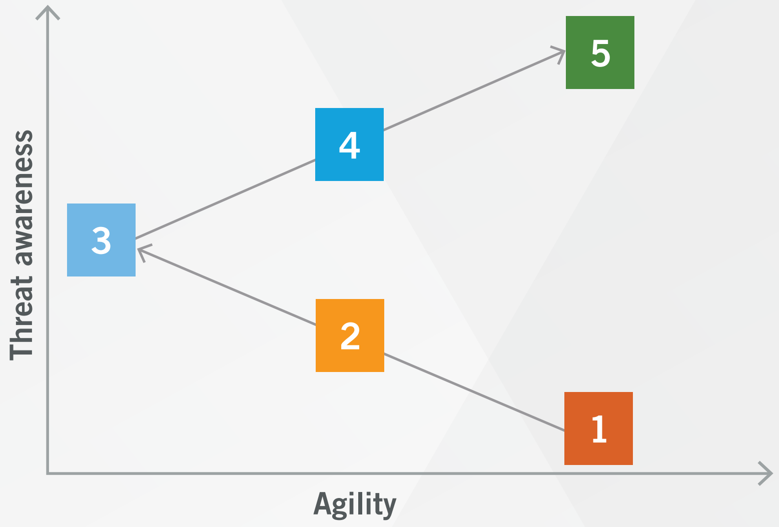
It is important to consider incident response maturity and capabilities in relation to threats relevant to the business and the scope of impact these threats can create. Business risk awareness requirements define metrics and security spend to achieve appropriate response times.

James Webb, CISO of Appalachian State University, proposed an incident response maturity model on a time axis, which Vectra has adopted and evolved as part of its advisory security practice. This model considers two core capabilities that are critical to incident response success:

Threat awareness/visibility – The ability to have accurate and reliable information about the presence of threat actors, their intentions, their historical activities, and how defences relate to them. Time-to-detect and time-to-understand are crucial dimensions to threat awareness.

Response agility/performance – The ability to quickly and sufficiently isolate, eradicate and return the FSI back to normal operations. This centres around the required time-to-respond.

Many security maturity frameworks imply the adoption of tools to provide linear capabilities as a layered "defence in depth" security approach. That methodology potentially leads to overlap and redundancy, which often has a negative impact on threat awareness and response agility. It also highlights trade-offs between detection and response capabilities that occur at every level of maturity. By relating these two attributes to the incident response process, maturity and capability can be defined and measured across the five stages of the maturity model based on the desired level of risk awareness.



Maturity	Typical Detection	Typical Response	Risk Awareness
Predictive Defense	Internal (Hunting, Deception) + External	Highly Proactive	Very High
Intelligence Driven	Internal (Hunting) + External	Threat/Adversary Driven	High
Process Driven	Internal (Hunting) + External	Service Driven (SLAs)	Medium
Tool Driven / Signature Based	External	Tool Driven	Low
Reactive / Ad-hoc	External, User Report	Reformat, Reinstall, Restore	Very Low

Develop visibility and agility for effective incident response

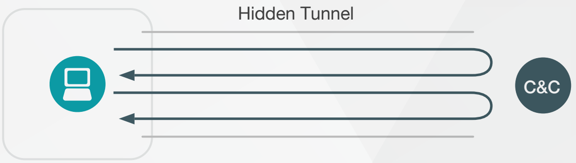
Defensive controls aren't perfect. Recent analysis in the M-TRENDS 2021 report identified that in 2020, threat actors hide inside organisations and operate with impunity for a median of 24 days before discovery. "Noisy" attacks such as ransomware, along with continued improvement in detection and response capabilities have seen attacker dwell times continue to trend downwards year on year. However, non-ransomware investigations showed an increase of 87.5%, rising to 45 days median dwell time. This shows that there's no room for complacency as motivated, persistent attackers continue to inflict significant damage through extended operations before being discovered. According to a SANS institute incident response survey, 62% of detected incidents resulted in a breach of information, devices or systems[2].

> "With Cognito, I can focus on the highest-risk threats. With other solutions, I have to filter to get rid of hundreds or thousands of false positives."
>
> **Matthias Tauber Senior Services Manager for IT Security DZ BANK**

Visibility and agility are the foundation of effective incident response. Slowing down attackers is only part of the challenge. It is vital to speed-up defenders, too. FSI organisations must quickly detect, understand, respond, and recover from attackers who get inside cloud, data centre, IT, and IoT networks. Every cloud service, data centre, networked device, and user within the FSI organisation forms part of an attack surface. Many component entities, such as IoT devices, also have little or no direct security controls or monitoring. Cloud, data centre, IT, and IoT networks provide vantage points across the infrastructure that advanced attackers will penetrate and spread. But the volume of data and ratio of the attacker signal-to-communication noise means that manual analysis and detection cannot provide the necessary scale, speed or efficiency.

[2] SANS 2019 Incident Response (IR) Survey: It's Time for a Change

Hidden Tunnels in FSI



Vectra analysis of live NDR deployments has identified vulnerabilities posed to financial services organisations. Compared to many industries FSI invest heavily into their security controls, often shutting down unused pathways, protocols and services. This has a forcing function on attackers who have to use the "lay of the land" and create hidden tunnels within legitimate protocols and services, including encrypted communications to surreptitiously access and steal data.

Analysis of hidden tunnels detected inside FSI Vectra NDR deployments revealed their use for both Command and Control (C2) and Data Exfiltration within common protocols such as HTTP, HTTPS an DNS. Such NDR detection did not require any decryption or deep packet inspection, instead using AI powered behaviour analysis targeting specific attacker techniques.

Vectra detected significantly more hidden command-and-control tunnels per 10,000 monitored devices in financial services than all other industries combined. There were also more than twice as many hidden data-exfiltration tunnels in financial services.

“Cognito for Office 365 is a windfall in light of how attackers are compromising and taking over accounts. As a long-time Vectra customer, I have confidence in identifying and stopping privilege escalation and account takeovers in Office 365.”

John Shaffer CIO Greenhil, Investment Bank

Understand attacker behaviours seen inside FSI

Vectra’s Cognito NDR platform is helping many financial service organisations around the globe secure their systems. By using AI to automate threat detection and incident response, the Cognito NDR platform enables financial service organisations to condense days, weeks, and months of manual security investigations into minutes. This allows IR teams to take immediate action to prevent damage and theft of their data.

By analysing anonymised metadata shared from hundreds of Cognito NDR platform deployments, Vectra has identified attacker behaviour insights that expose tactics that remain open to abuse. In many cases, these tactics cannot be completely blocked without imposing material damage on legitimate operations, so early and effective detection and response is essential.

“Vectra contextualises everything, reducing the number of alerts and pinpointing only the things of interest. This is a key feature for me. Because of this, a non-trained analyst can use it almost right away.”

Security Manager, Financial Service Firm

MFA bypass in Azure AD / M365

Research published in the Vectra Spotlight Report for Office 365 identifies the tools and services within the cloud-based application commonly being leveraged by attackers. By observing 4 million Office 365 accounts over a 90-day period, we were able to identify suspicious high-risk behaviours associated with attacker techniques exploiting built-in Office 365 capabilities.

Vectra identified 87% of monitored customer deployments exhibited suspicious sign-on activity which used Azure Active Directory or OAuth. OAuth is an open standard for access authentication, often utilised by third-party applications to authenticate users by employing Office 365 login services and the user’s associated credentials. The OAuth authorisation code grant can be used in apps that are installed on a device to gain access to protected resources, such as web APIs. Attackers are leveraging OAuth enabled malicious Azure applications to maintain persistent access to users’ Office 365 accounts and other MFA gated services.

Understanding observed attack behaviours from within FSI provides a valuable contribution to the intelligence-based threat modeling and definition of requisite associated security controls. These behaviours, the tactics, techniques and procedures (TTP) can also be mapped back to industry frameworks and knowledgebases such as the well-respected MITRE ATT&CK matrices. By focusing on the immutable behaviours that attackers must manifest, you create security controls that have broad coverage and longevity. This unlike traditional fragile signatures, which are used to find a singular piece of malicious code or a piece of known attacker infrastructure.

Train hard, fight easy (and pass pen tests)

The military adage “train hard, fight easy” has never been more appropriate for security incident responders. All the technology in the world can’t help in the absence of situational awareness, organisational context and the ability to work cohesively and effectively as part of a team. Just like real attacks, external penetration tests begin unannounced, almost always initially undetected and only create subtle signals hidden within the cacophony of legitimate communications and the distracting noise of benign and low severity security alerts.

“When we do have pen testers come in, we can see quite clearly how Vectra pick traffic up and how it develops from a small or medium alert to go to higher severity, then how it adds all those events together to give more visibility.”

Head of Information Security at an insurance company

Using behavioural detection approaches provide a different kind of signal to incident responders, one that surfaces high risk behaviours rather than black and white detection signatures of explicit threats.

Vectra’s AI powered Cognito NDR augments the defending “blue team” with high-fidelity attacker TTP behavioural detections which are prioritised by risk/certainty index™, profiled by attack type and the totality of the affected hosts and accounts are displayed as attack campaign. Security insights and history of affected accounts and hosts are also made available. This enables the IR analyst to quickly understand what is happening and quickly respond. Analyst average workload reductions of 34x have been observed in live Vectra Cognito NDR deployments.

However, even highly actionable information still requires the analyst to make the right decision and take appropriate intervention in a timely manner. Some response actions, such as host isolation may be automated, possibly even autonomised against some criteria but the role of human analysts remain the central pillar of value in security operations workflows.

The ability to think like an attacker aids quick formation of understanding and anticipation of next steps. Likewise, building experience of running an incident response through detection, investigation and remediation builds valuable muscle memory, and can highlight training needs and procedural weaknesses.

Great tooling and workflows alone are insufficient. Regular practice through exercises, lab sessions and scenario workshops set a security program up for success. Military forces train regularly to hone their skills so that in the confusion of conflict they are able to operate with predictability and effectivesness. High performance incident response teams take the same approach.

Workshop Type	BLUE TEAM WORKSHOP	RED TEAM WORKSHOP
Workshop Scope	Vectra Blue Team Workshops put you on the front line of defence as you investigate an incident that occurred at a government spy agency. You'll obtain a first-hand look at a real-world incident through the lens of a network detection and response (NDR) solution. We'll help you sharpen your analysis, hunting, and defending skills in a simulated enterprise environment with the Vectra Blue Team Workshop. Follow a step-by-step, moderated path as you analyse a real-world advanced attack and pick up CPE credits while you are at it. Vectra Blue Team Workshop helps individuals better understand how to analyse behaviour-based indicators that occur post-compromise. Analysing evidence without signature matching requires a different way of logical thinking and assessment. No special tools are needed as this hands-on workshop provides a step-by-step narrative from start to finish. This private workshop is a way for you to gain free hands-on, interactive, virtual training to broaden your incident response skills.	Vectra Red Team Workshops are an educational lab where FSI security practitioners can better understand the skills and tactics of the adversary. Participants will learn about critical attack vectors and how attackers plot, ploy and work their way into enterprise network and cloud vulnerabilities. Participants will then take the training wheels off for open play as a "Red Team" attacker. Attendees will reconvene for a working session, walking through the live attacks from the morning and how blue teams, or the threat hunters, actually identify, detect, and respond to advanced threats. This virtual private workshop is an excellent way to "think like and attacker". Available as a standalone this is an ideal follow on to a Vectra Blue Team workshop to help build a flexible "Purple Team" mindset.
Participant Requirements	• Skill Level: Basic incident response experience (e.g. Managing SIEM or other detection tool alerts) • A Windows, Mac or Linux desktop • VPN Client	• Skill level: Basic attacking skills (i.e. Threat Hunters, Security Analysts, etc.) • A Windows, Mac or Linux desktop • VPN client installation • Completion of preparatory set up and registration tasks
Certification (ISC)² CPE SUBMITTER	3.5 CPE credits and a digital certificate upon completion.	3.5 CPE credits and a digital certificate upon completion.
Eligibility	Private Vectra Blue Team and Red Team Workshops are complimentary to security practitioners working for existing Vectra customers or FSI organisations considering NDR solutions.	

Conclusion

With finite resources available to security programs, NDR is playing an increasingly important role in securing FSI. Security teams must adopt an assumed-compromised mindset and focus on early detection and response to advanced attackers.

FSI around the world are using Vectra to mature their incidence response capability and improve their performance in compliance driven penetration tests by:

- Threat intelligence that informs FSI's own threat modelling
- Automated detections that are risk prioritised, high-fidelity threat detections that, are delivered with contextualised insights
- Accelerated response actions through feature-rich Vectra integration with wide range of security tools including popular SEIM, SOAR and EDR vendors
- IR analyst skills development through action-based learning workshops with blue team and red team education exercises

The AI-powered Cognito NDR platform from Vectra enables FSI security teams to identify and respond faster to hidden threats in cloud, data centre, IT, and IoT networks. Vectra helps FSI security leaders reduce the risk of a breach, improve the efficiency of their security operations, help to ensure compliance, and extend cybersecurity to the cloud. To find out more visit vectra.ai.

For more information please contact us at info@vectra.ai.

> "We went from zero to 100 percent visibility into attack behaviours with Vectra."
>
> **Head of security Global financial services firm**

About Vectra

As a leader in network detection and response (NDR), Vectra® AI protects your data, systems and infrastructure.

Vectra AI enables your SOC team to quickly discover and respond to would-be attackers —before they act. Vectra AI rapidly identifies suspicious behavior and activity on your extended network, whether on-premises or in the cloud.

Vectra will find it, flag it, and alert security personnel so they can respond immediately. Vectra AI is Security that thinks®. It uses artificial intelligence to improve detection and response over time, eliminating false positives so you can focus on real threats.

Email info@vectra.ai vectra.ai