VECTRA
SECURITY THAT THINKS®

SOLUTION BRIEF

How financial institutions can stop cyberattacks in their tracks

The biggest target

It's no surprise that financial services institutions (FSIs) remain the top target for cybercriminals. In 2020, the financial sector had 1,509 incidents with 448 confirmed data disclosures, according to the 2020 Verizon Data Breach Investigations Report.

Banks, credit unions, credit card companies, insurance companies, consumer finance companies, investment firms and stock brokerages offer rich pickings in terms of actual money and personally identifiable information (PII).

While PII and PHI remain popular targets, attackers are finding it more profitable to go straight for the money using sophisticated advanced persistent threats (APT), such as Carbanak, as well as ransomware. During the two-year Carbanak campaign, attackers infiltrated more than 100 banks across 30 countries and were able to steal an estimated $1 billion.

Attackers are finding it more profitable to go straight for the money using sophisticated advanced persistent threats (APT), such as Carbanak, as well as ransomware.

HIGHLIGHTS

- The majority of attacks (64%) against FSIs are perpetrated by external actors who are financially motivated (91%) to access easily monetized data stored by the victim organizations.
- Security and IT staff are forced to manage two critical priorities: Stay on top of cyberattackers while also meeting an array of regulatory and compliance requirements.
- Leveraging a unique combination of data science, AI-derived learning and behavioral analysis, the Cognito® network detection and response (NDR) platform from Vectra® identifies all phases of an attack, including C&C communication, internal reconnaissance, lateral movement, data exfiltration, and botnet monetization.

The majority of attacks (64%) in this sector are perpetrated by external actors who are financially motivated (91%) to access easily monetized data stored by the victim organizations, according to the 2020 Verizon report. And the nature of attacks breaks down as personal (77%), other (35%), credentials (35%), and bank breaches (32%). No wonder the chair of the U.S. Securities and Exchange Commission (SEC) has stated that cybersecurity is the biggest risk facing the financial system. Cyberattacks against FSIs are becoming increasingly frequent and sophisticated, and costs of breaches continue to rise.

Security teams are forced to manage two critical priorities that compete for time and resources. Teams must simultaneously stay on top of cyberattackers while also meeting an array of regulatory and compliance requirements. In addition, emerging threats from technologies, such as the adoption of Internet-of-Things (IoT) devices, are stretching security staff to their limits.

Vectra offers FSIs a new and stronger class of security solution that finds threats before they inflict damage.

Combining data science, AI-derived machine learning techniques and behavioral analysis, the Cognito NDR platform from Vectra automates the detection and response to in-progress cyberthreats in every phase of the attack lifecycle.

Cognito also augments security staff by providing a level of intelligence that focuses attention on actual attack behaviors so security teams can act quickly instead of manually hunting for threats.

Challenges facing FSIs

The financial services industry has some of the most robust security infrastructure of any industry, and has used techniques such as machine learning for decades to detect fraudulent behavior. Despite this, the industry faces a number of challenges in protecting its assets, which are highlighted below.

Challenge: The endless onslaught of attacks

FSIs offer lots of goodies to steal and consequently are the targets of a wide range of cyberattacks, including:

- Malware, including ransomware
- Persistent attacks that infiltrate to steal funds or trade secrets
- Hidden command-and-control (C&C) communication by remote attackers
- Botnet and zombie attacks
- Man-in-the-browser techniques that defraud banking customers

Attacks using one particularly nasty type of malware, ransomware, have become rampant in enterprise organizations. Ransomware now accounts for 27% of malware incidents, and 18% of organizations blocked at least one piece of ransomware, according to the 2020 Verizon report.

Cyberattackers will attempt to infiltrate FSIs in a variety of ways:

- Through customer-owned computing devices
- Third-party providers such as check/payment processors, trading and settlement operations, and data processing companies Via direct attacks against bank employees and assets
- Via direct attacks against bank employees and assets

Banking customers have long been the target of botnets such as Zeus and Carberp, which enable cybercriminals to infect customer computers in order to steal login credentials and exfiltrate money or to manipulate online banking sessions to steal funds.

More recently, attackers have turned their sights on FSIs themselves, targeting them directly with APTs, ransomware and other mechanisms, including exploiting remote access tools, such as the Ammyy remote administration, that are commonly used by bank administrators.

As the Carbanak APT attack on SWIFT payments and other high-profile cyberattacks against FSIs have shown, attackers are persistent and will use any means necessary to steal money, PII and other valuable assets.

The theft of PII is associated with financial fraud, enabling cybercriminals to open new lines of credit and file fake tax returns. Perpetrators also use PII to create tailored phishing lures and to launch other social engineering attacks.

Attackers are also branching out by launching new types of threats. For example, the Dridex group added ransomware to its portfolio, leveraging the distribution operations used to support Dridex to also spread Locky, a type of ransomware.

A key challenge for FSIs is the rapidly changing nature of attacks. Verizon research shows 70-90% of malware samples are unique to a single organization. Perpetrators introduce simple modifications into their malware code so that the hash is unique, yet the malware exhibits the same desired behavior. These slight modifications make it easy to avoid detection by signature-based security tools.

Likewise, attackers are employing sophisticated evasion techniques once they are inside a network. By using tools commonly used by bank administrators, including VNC, PuTTY and Ammyy, Carbanak attackers avoided detection for extended periods of time. Stealth and persistence have become key strategies for attackers.

The persistent, internally driven network attack has become the norm, and security products, teams, and processes need to adapt accordingly.

In fact, such operations can span months, starting when employees are initially infected via phishing or watering hole vulnerabilities, progressing slowly as attackers use ongoing remote control to perform reconnaissance and move laterally to extend their footprint, and concluding when they steal data, money or other assets.

With the proliferation of IoT devices connected to networks, FSIs also anticipate that IoT devices will become a vector for attacks. Sensors to monitor ATMs are becoming common, enabling a bank to shut down an ATM in the event of a security issue. IoT devices pose privacy as well as security issues that FSIs will need to address.

The solution

The persistent, internally driven network attack has become the norm, and security products, teams, and processes need to adapt accordingly. Given how rapidly perpetrators modify their malware and other attack mechanisms – and the growing use of APTs – FSIs need a network security solution that identifies and stops attacks in progress.

Security teams need a real-time, automated NDR that has visibility into the behavior of all traffic and host devices on the network, including IoT and BYOD devices, and can detect every phase of a cyberattack, such as C&C communication, internal reconnaissance, lateral movement and exfiltration.

Such a network security solution is needed to fill in the gap between current security tools that only focus on prevention at the network perimeter and the post-attack forensic clean-up phase after assets have been compromised.

Prevention tools at the network perimeter, such as next-generation firewalls, IDS/IPS and malware sandboxes, help keep known threats out of FSI networks. But new, unknown attacks easily evade perimeter security that are blind to reconnaissance, lateral movement and other attack behaviors that cybercriminals use to map out the target network and spread to additional hosts.

Likewise, malware sandbox technologies provide a very incomplete approach to managing APTs. Keep in mind that the success of Carbanak largely depended on its ability to infiltrate a bank's network and remain undetected as the attack progressed inside the network. And unlike a sandbox, which briefly looks for infecting behavior in a virtual environment, it is important to constantly monitors all behavior in real time on the internal network.

Furthermore, an employee or contractor device can be compromised offsite while the user is on a guest Wi-Fi network and that exploit spreads when the user connects the infected device at work. Security teams must detect attacks in progress in real time, pinpoint the compromised host devices, and alert staff to take action.

Challenge: Meeting compliance and regulatory mandates

Financial institutions face a wide range of compliance requirements from numerous regulatory bodies, so it's understandable that compliance remains a top reason for securing sensitive data.

In the United States, FSIs must demonstrate compliance with federal regulations such as the Dodd-Frank rules and those from agencies such as the SEC, Financial Industry Regulatory Authority, and the Federal Financial Institutions Examination Council.

Likewise, each state has its own regulators for banks, insurance and securities as well as its own laws, including data breach laws. In Europe, FSIs must comply with regulations from the European Banking Authority, GDPR and other agencies.

The challenge for FSI staff is to demonstrate compliance with a wide range of regulations from a variety of regulatory bodies, each of which chooses the particular framework that they want to use when performing an audit or sweep.

Regulators often focus on particular issues based on what security events and cyberattacks are happening at the time. For example, after a wave of ransomware attacks, regulators may want to focus on malware controls and data backup and recovery.

The combination of many regulatory bodies, many standards, and the changing threat landscape means that security teams never know exactly what questions regulators will ask. Consequently, there is no single report to generate.

Instead, security and compliance teams must be able to document on the spot what specific controls are in place based on the specific questions posed. And they typically turn to several sources to pull the requested data, which can be a time- consuming process.

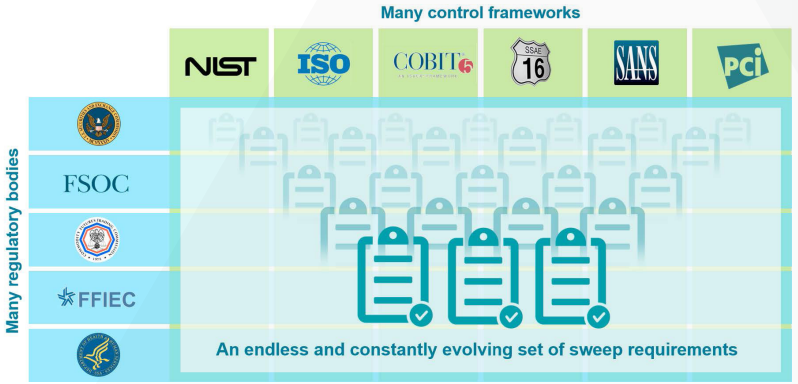

Figure 1: Inside the regulatory tornado

The solution

FSIs need an NDR platform that allows them to quickly and easily respond to unique compliance questions. In order to quickly pull up requested compliance data, FSIs need a security solution that consistently monitors all network traffic, both internal and to/from the internet, and including cloud and data center workloads, hosts, user accounts, and IoT and BYOD devices.

Comprehensive visibility into all cloud and data center workloads, hosts, user accounts, and IoT and BYOD devices and their behaviors is necessary to document compliance for a broad range of technical controls, from asset tracking and security incident reporting to data-loss prevention, and to prove the controls are working.

Challenge: Protecting assets in the age of encryption

Due to the critical need for privacy, the vast majority of traffic on FSI networks is encrypted, including stock trades, payments, transfers, and PII. While encryption provides a layer of protection for sensitive traffic, it also obscures traffic from many network- based security solutions – something attackers are well aware of.

Unfortunately, a growing number of sophisticated attackers are employing a variety of encryption methods – from standard SSL/TLS to more customized schemes – to hide their malicious code and activities, especially their C&C and exfiltration traffic. In addition, the use of hidden tunnels is on the rise, with attackers preferring HTTPS to other protocols for constructing hidden tunnels.

Although some organizations use man-in-the-middle techniques to decrypt outbound traffic for inspection, FSIs often don't have that option due to strict privacy laws that prohibit inspection of encrypted customer records and other user traffic. Decrypting traffic also extracts a heavy toll on application performance, making it unpopular with users.

Additionally, many online service providers, including Google, undermine the use of certificate pinning, a technique that enterprises increasingly use to thwart man-in-the-middle attacks on web sessions.

In an attempt to deter attackers who have stolen valid certificates, Google and other providers choose to trust only certificates from a specific trusted root certificate authority instead of any recognized certificate authority. This breaks the man-in-the-middle decryption methods used by many security teams.

The solution

To deal with encrypted threats, FSIs need a way to detect malicious attack behaviors without decrypting packets and inspecting the payload.

This requires a new approach to network security based on analyzing traffic behavior and patterns to reveal fundamental attacker behaviors hidden within network traffic, even encrypted traffic, across all applications.

Advanced behavioral analysis is needed to identify and monitor hidden tunnels, data leaving the environment, malware receiving C&C instructions, remote attackers using remote access tools, and attackers delivering malware updates.

For example, behavioral traffic analysis can quickly distinguish between human and machine-driven traffic. This can expose an attacker using a remote administration tool by revealing that what appears to be an end-user connection is actually being remotely controlled by an outsider.

Challenge: Security teams have a lot on their plates

The majority of security products create work for IT, requiring staff to sift through many thousands of alerts to identify real threats. In many networks, it's common to get 50 alerts per minute.

Faced with lean security teams, it's not humanly possible to sift through and interpret those vast volumes of data, identify the most serious threats, and then mitigate attacks before they spread and do damage.

Complexity and a shortage of skilled cybersecurity personnel have always been significant barriers to wider adoption of data security tools and techniques. The chronic and growing skills shortage continues to be a problem across the industry.

The solution

FSIs need security solutions that reduce the work for overburdened security teams instead of creating more work. This requires solutions that are comprehensive, easy to deploy, and automate real-time threat detection, response and reporting.

In particular, security teams need a solution that streamlines operations by condensing the vast amounts of security-related data down to simple, actionable information, focusing staff attention on actual attacks in progress by pinpointing the physical devices at the center of an attack and alerting staffs about high threat activity.

The Cognito NDR platform is instrumental in helping FSIs address the security, compliance and manpower challenges they face.

The Cognito NDR platform detects and responds to attacks in progress, streamlines operations

The AI-driven Cognito NDR platform helps FSIs detect and respond rapidly to threats, before any damage is done. It picks up where perimeter security leaves off by providing deep, continuous analysis of internal and internet network traffic and detecting the fundamental actions and behaviors that attackers perform when they spy, spread across FSI networks and steal valuable assets.

Leveraging a unique combination of data science, AI-derived learning and behavioral analysis, the Cognito NDR platform detects all phases of an attack, including C&C communication, internal reconnaissance, lateral movement, data exfiltration, and botnet monetization.

The Vectra Threat Certainty Index™ automatically consolidates all detections and assigns scores that indicate in real time which hosts pose the greatest risk, enabling FSI security teams to immediately focus on the highest risk detections.

The Cognito NDR platform also learns about the naturally occurring behavior patterns in an FSI network and provides a visual map of the relationship between threats, hosts and key assets.

This makes the Cognito NDR platform instrumental in helping FSIs address the security, compliance and manpower challenges they face.

Address today's dynamic threat landscape

The Cognito NDR platform monitors all network traffic from all devices – internal traffic within the network as well as traffic going to and from the internet. It also works across all cloud and data center workloads, hosts, user accounts, and IoT and BYOD devices.

The Cognito NDR platform analyzes traffic using a combination of AI-derived learning, data science and behavioral analytics to detect the attack behaviors of known and never-before-seen threats at any stage across the entire attack surface of an organization. All detections are automatically scored and correlated to quickly prioritize the threats so security teams can promptly stop the attack and mitigate its impact.

What is unique about the Cognito NDR platform is that it uncovers the fundamental behaviors of cyberattacks, such as internal reconnaissance, the internal spread of malware, abuse of account credentials, data exfiltration, ransomware activity, and a wide variety of C&C and other hidden communications.

For example, the Cognito NDR platform has multiple ways to identify ransomware in action, including detecting:

- C&C communication
- The malware update of ransomware binaries on infected hosts
- The internal searching and scanning of file shares
- The theft of credentials to escalate privileges
- The ransomware file encryption activity itself

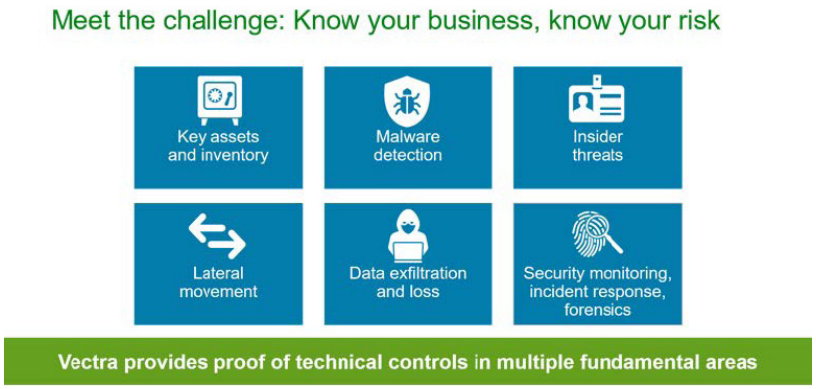

Figure 2: Meet the challenge: Know your business, know your risk

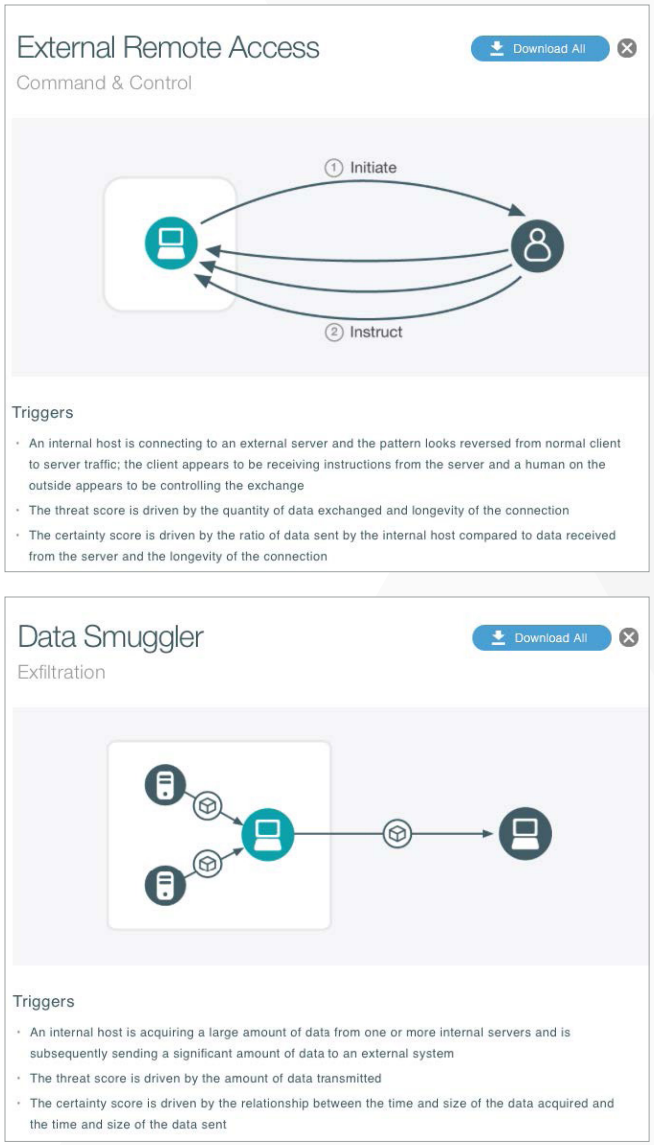

Figure 3: Simple detection explanations: Evidence of technical controls

Because the Cognito NDR platform recognizes patterns of traffic, there's no need to crack open packets to see what's inside, preserving data privacy for encrypted traffic. The Cognito NDR platform uses mathematical models and performs a highly sophisticated analysis of network traffic to detect the presence of hidden tunnels within HTTP, HTTPS and DNS traffic – without requiring any type of encryption whatsoever.

Similarly, the Cognito NDR platform uses data science and AI-derived machine learning to identify the presence of external remote access, even malicious remote access tools that are customized or previously unknown to the security industry.

Streamline operations and save staff time

Understanding that IT and security staff time is at a premium, the Cognito NDR platform is designed to be easy to deploy and to use. Automation plays a pivotal role.

The Cognito NDR platform automates the tedious part of a Tier 1 security analyst's job, empowering security teams by condensing vast amounts of data down to simple, actionable answers that save time, effort and money.

This automation offers two benefits – staff can perform investigations in less time and non-expert staff can handle more investigations. Vectra customers have reported 75-90% reductions in time spent on investigations, and have successfully deferred analysis to IT generalists instead of escalating incidents to higher paid experts.

The Cognito NDR platform pinpoints physical hosts at the center of an attack and automatically tracks and scores threats in context over the full duration of the attack, displaying alerts on the Threat Certainty Index so security teams instantly know which hosts, accounts and workloads with attack indicators pose the most significant risk and highest degree of certainty.

Details about an attack are just one-click away, enabling staff to easily view the exact packets between the compromised host and other internal assets it is attacking or external parties with which it is communicating, and respond accordingly.

The Cognito NDR platform also enables security teams to mark proprietary databases, credit card databases, financial records and other critical assets so they can see threats in the context of vital assets and predict the potential impact of an attack.

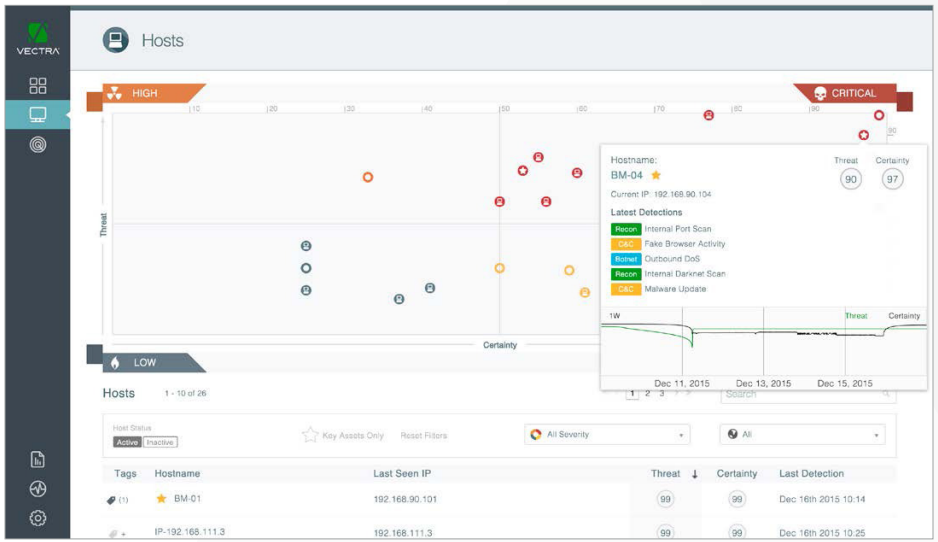

Figure 4: The Cognito NDR platform pinpoints physical hosts at the center of an attack and automatically tracks and scores threats in context over the full duration of the attack

In addition, the Cognito NDR platform makes it easy to share threat intelligence with other team members and systems. Security teams can be automatically notified via email when devices reach specified threat or certainty score thresholds.

And finally, a robust API allows the Cognito NDR platform to integrate with other third-party security solutions, such as SIEMs, next-generation endpoint security, traffic optimization, and next-generation firewalls. For example, Syslog and Common Event Format (CEF) log integration provides SIEMs with precorrelated Vectra detections and host scores.

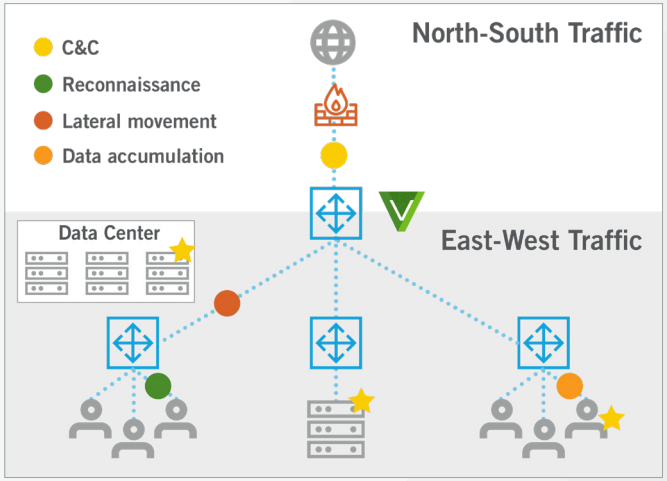

Figure 5: Full visibility ensures knowledge of business risk

Passive internal deployment

- Leverages TAP or SPAN
- E-W and N-S visibility of traffic
- Sees all phases of behavior

Persistently tracks all devices

- Any OS, BYOD, IoT

Protects without prying

- Behavioral models find threats without looking into the payload
- Find threats in SSL without decryption

The Cognito NDR platform makes it easy to share threat intelligence with other team members and systems.

Deliver compliance data on demand

With full visibility into all traffic and the ability to detect any phase of an attack, Cognito is an ideal platform to document compliance for a broad range of technical controls.

The Cognito NDR platform delivers clear, intuitive analysis with one-click access to all supporting evidence, allowing staff to quickly and easily respond to any data request from regulators.

While persistently tracking all critical assets and reporting on them, the Cognito NDR platform makes it easy to maintain a compliance trail. Likewise, because it monitors and detects hidden tunnels and data exfiltration behaviors used by attackers, it's easy to document compliance efforts for data-loss prevention.

With the Cognito NDR platform, a powerful reporting engine lets security teams generate reports on the fly as well as schedule specific reports to be compiled on a regular basis. Reports can focus on any timeframe, section of the network, and host or detection. Advanced filtering capabilities can be used to highlight specific data, such as all hosts with threat certainly scores above 50.

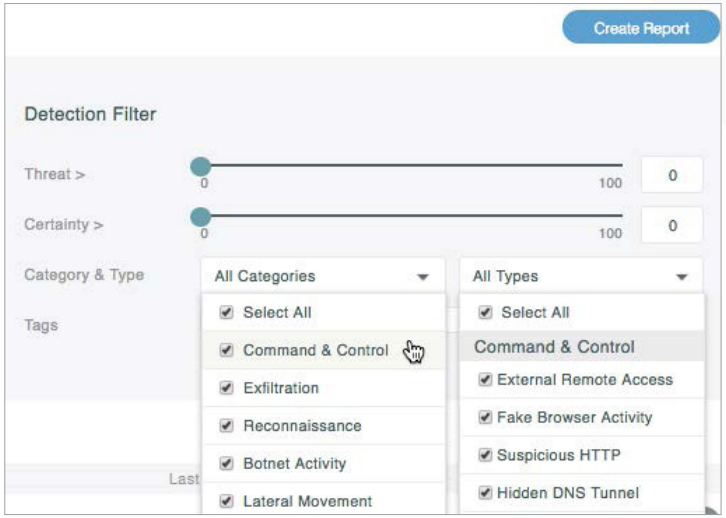

Figure 6: Easily document controls based on type of threat

← Filter events based on threat level

← Easily report on controls specific to any phase of attack:

- Malware behavior
- Lateral movement
- Data loss

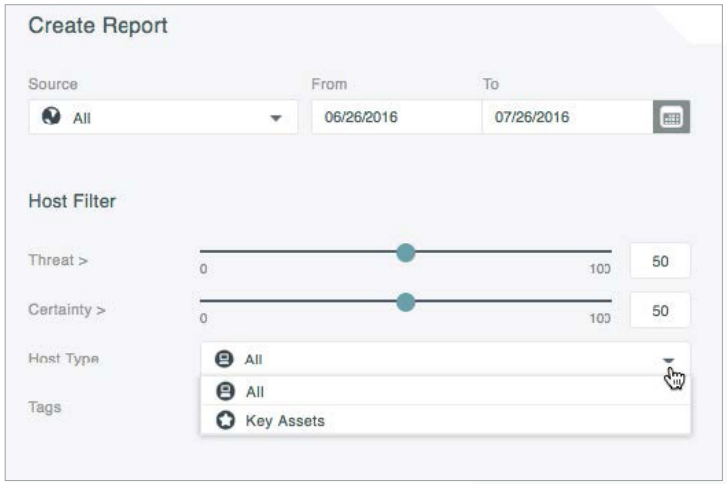

Figure 7: Track and document any and all hosts in your network

Persistently tracks all devices regardless of device type or OS

← Report on all hosts or those with particular risk levels

← Report on all hosts, key assets, or any custom category

A powerful solution to combat modern threats

FSIs will continue to be a top target of cyberattacks. Vectra arms security teams with an AI-driven NDR platform that works in real time to rapidly detect known and unknown cyberattacks across the constantly evolving threat landscape.

With the unique ability to detect and mitigate cyberattacks while they are happening, the Cognito NDR platform enables security teams to respond with unprecedented speed, accuracy and efficiency – well before the bad guys cause irreparable damage and public embarrassment.

Likewise, the Cognito NDR platform gives security teams unparalleled network visibility into malicious attack behaviors and automates the hunt for cyberthreats, which enables security teams to quickly and easily respond to audits and have more time to focus on keeping critical assets safe.

The Cognito NDR platform gives security teams unparalleled network visibility into malicious attack behaviors and automates the hunt for cyberthreats, which enables security teams to quickly and easily respond to audits and have more time to focus on keeping critical assets safe.

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai