VECTRA®

Protecting higher education networks from cyber threats

Real-time, automated threat detection and response finds attackers before damage is done

Higher education is one of the most targeted sectors

Thanks to their open, collaborative environments and a treasure trove of high-value assets, universities and colleges have become a top target of data breaches and cyber attacks. Higher education ranks second only to the medical industry in its volume of data breaches, according to The Privacy Rights Clearinghouse.

A key goal of higher education institutions is to facilitate the free exchange of information. Consequently, campus IT systems are relatively open, supporting thousands of entitled users, most of whom bring their own devices to campus. Students (and many staff) tend to adopt the latest applications and technologies, use social media, and share lots of files.

In addition, higher education generates and collects a vast array of data from students, faculty, staff and visitors. This includes personally identifiable information (PII) such as names, birth dates, and Social Security numbers; financial data relating to tuition fees and student loans; protected health information (PHI); enterprise data; and operational data, such as grade management systems and research.

With their open networks, large volumes of data and freedom of access, higher education institutions present an expansive and porous attack surface that exposes them to a variety of cyber threats and risks. It's estimated that a higher education institution is breached each week.

Organized criminals are behind most breaches, although students and other parties sometimes attack institutions to damage their reputation or highlight security weaknesses. In addition, organized criminals, nation states and unscrupulous corporations engage in international and industrial espionage.

Research institutions have considerable intellectual property to poach, such as data that could lead to a valuable new product (e.g., a new drug) or has significant value to government agencies. For example, Pennsylvania State University's engineering department was the target of a multi-year cyber attack tied to a foreign actor focused on acquiring research used by the U.S. Navy. At one point, the attack debilitated the university's network for three days.

The escalation of attacks presents serious challenges for higher education. Security and IT staff are forced to manage critical priorities that compete for time and resources. Security teams must simultaneously stay on top of cyber attackers while maintaining open access and also meeting an array of regulatory and compliance requirements.

Vectra® offers higher education institutions a new, completely automated class of security solution that finds cyber attackers inside networks in real time before they inflict damage. Combining data science, modern machine learning techniques and behavioral analysis based on artificial intelligence, the Cognito™ automated threat detection and response platform detects every phase of an in-progress cyber attack.

Cognito also augments security staff by providing automated Tier 1 analysis and intelligence that exposes actual attack behaviors so security teams can act quickly instead of manually hunting for threats.

Challenges facing higher education institutions

Higher education campuses are like small cities, with many students living on campus, a variety of vendors providing services, and lots of visitors. This environment gives cyber attackers numerous ways to successfully infiltrate higher education networks.

In a recent analysis of data breaches that disclosed personal information, the education sector accounted for 1.35 million identities exposed in one calendar year alone.

Institutions large and small, public and private, have been targeted worldwide. For example, the University of California, Berkeley reported a major breach in early 2016 involving financial data of 80,000 students, alumni, current and former employees, and vendors whose information was in the system. This was the school's third breach in 18 months.

The University of Central Florida also suffered a large-scale data breach in 2016, which compromised the personal information of some 63,000 current and former students, faculty and staff. Post-breach forensic analysis indicated that attackers were focused on collecting Social Security numbers.

Institutions that had major breaches in 2015 include Harvard University, Washington State University, Johns Hopkins University, the University of Connecticut, and the University of Virginia.

Among the greatest threats are:

- Persistent attacks that infiltrate networks to steal or damage sensitive data, including PII, PHI, and payment card data as well as intellectual property and research data.
- Malware, including ransomware.
- Hidden command-and-control (C&C) communication by remote attackers.
- Botnets, zombie attacks and other threat vectors.

Cyber attackers are successfully infiltrating higher education networks in a variety of ways, including:

- Direct attacks against students, academics, administrators, employees and assets, including BYOD and IoT devices.
- Through smartphones and computers that visitors bring onsite.
- Via third-party providers, such as food services and maintenance companies, that contract with higher education institutions.

Cyber attacks will continue because they are lucrative for attackers. Unfortunately, they are costly to higher education institutions, averaging $225 for each compromised record, according to the Ponemon Institute.

Key attack vectors

Just a quick look at some recent breaches highlights the scope of the challenges facing higher education institutions.

Phishing scams on the rise

Colleges and universities are reporting increased spear-phishing incidents in which hackers send personalized, legitimate-looking emails with harmful links or attachments.

For example, early in 2016, current and former employees of Tidewater Community College (TCC) in Virginia had their personal information stolen in a tax season phishing scam. An employee in the school's finance department received a request from a fake TCC e-mail address asking for all employee W-2 information.

Not realizing the e-mail was fake, the employee responded with sensitive information including names, earnings, and Social Security numbers. Consequently, at least 16 TCC employees reported that false tax returns had been filed under their Social Security numbers.

Ransomware attacks

For criminals, ransomware is a fast and easy attack with a bigger payout than stealing PII or credit cards, both of which have a declining value as time passes after their theft. Hackers are increasingly employing ransomware to lock up an organization's data, holding it until a ransom is paid, often in nearly untraceable Bitcoin.

A new survey of ransomware's spread among some 20,000 organizations in different industry sectors found that education is the biggest target right now, with one in 10 education organizations hit with ransomware. More than 11% of education organizations were hit by Nymaim and 4% with Locky.

Ransomware is a worldwide phenomenon. For example, in the last year universities in England have been hit hard by ransomware; Bournemouth University, which is home to a cybersecurity center, was hit 21 times in a recent 12-month period.

Fast, easy and offering an immediate payout for attackers, ransomware attacks are projected to increase 250% in 2016, according to the Beazley Breach Insights 2016 report.

BYOD vulnerabilities

One of the biggest sources of risk for higher education is the sheer volume of personal laptops, tablets, smartphones, and other devices that students, faculty, vendors and visitors bring with them to campus.

Many colleges and universities try to enforce student use of antivirus software, for example, but it's an uphill battle. The chances of a malware-infected device connecting to the network is high.

IoT exploits

In addition to BYOD, security staff in higher education must address the growing number of IP-enabled devices connecting to their networks. Like many enterprises, higher education institutions are looking for ways to leverage the intelligence of Internet-of-Things (IoT) devices to streamline facilities management and cut costs.

For example, smart water and energy meters and heating and air conditioning systems can lower energy costs, and provide remote access that can streamline repairs. To improve campus safety, many institutions are deploying security equipment such as cameras, access controls, and other monitoring devices that connect to the network.

In addition, students bring IoT devices onto campus, including gaming consoles and set-top boxes such as Apple TVs, along with personal devices such as iWatches and Fitbits.

Unfortunately, these IoT devices provide an easy entry point for cyber attackers who can then move laterally through a campus network in search of PII, PHI, sensitive research data, and other target assets.

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 launch other advanced persistent threats (APTs), higher education institutions need a network security solution that identifies and stops attacks in progress.

IT security teams need a real-time, automated threat hunting system that provides visibility into all traffic and host devices on the network – including BYOD and IoT devices – and can detect every phase of a cyber attack, such as C&C communication, internal reconnaissance, lateral movement and exfiltration.

Prevention tools at the network perimeter, such as next-generation firewalls, IDS/IPS and malware sandboxes, all help to prevent infection or compromise. But sophisticated attackers have repeatedly shown that they can evade these perimeter security products, whose basic technology is more than 25 years old.

To make matters worse, once attackers get inside the network, these solutions are blind to the reconnaissance, lateral movement and other threat behaviors that cybercriminals use to map out the target assets and spread to additional hosts.

Likewise, malware sandbox technologies provide an incomplete approach to managing APTs because they only briefly look for infecting behavior in a virtual environment. What security teams need is a solution that constantly monitors and analyzes all behavior in the network.

Detecting the tell-tale signs of cyber attackers is critically important when dealing with IoT devices, which can act as proxies for routing an attacker's traffic into, out of, and across the network. And as mentioned earlier, IoT devices cannot run endpoint security agents and will not be protected by IPS signatures.

Challenge: Meeting compliance and regulatory mandates

Institutions of higher education are subject to a variety of privacy regulations and other compliance rules, including:

- The Family Educational Rights and Privacy Act (FERPA), a federal law that protects the privacy of student education records. FERPA applies to all schools that receive funds under an applicable program of the U.S. Department of Education.
- The Health Insurance Portability and Accountability Act (HIPAA), which requires institutions to report a breach of PHI data.
- Payment Card Industry Data Security Standard (PCI DSS) regulations apply to higher education institutions that accept payment cards.
- The Safeguards Rule, set by the Federal Trade Commission, directs institutions providing financial products or services to establish a comprehensive written information security program containing administrative, technical, and physical safeguards to protect customers' personal information. The FTC has the power to investigate and bring enforcement actions against entities that failed to maintain appropriate data security standards in accordance with the Safeguards Rule.

Given their open environments, higher education institutions of every stripe face formidable data privacy and compliance challenges.

The solution

Higher education institutions need a security platform that allows them to quickly and easily respond to unique compliance questions.

Comprehensive visibility into the behavior of all network traffic associated with host devices 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.

Security and compliance teams should look for a security solution that continuously monitors all network traffic, both internal and to/from the Internet, from all devices, including BYOD and IoT, and lets them pull up requested compliance data on demand.

Challenge: Protecting assets in an age of encryption

Due to the critical need for privacy, higher education institutions are encrypting a growing volume of traffic on their networks, including student records, PII, PHI and payment data. 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, sophisticated attackers are also 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 cybercriminals preferring HTTPS over other protocols to conceal their attack communications.

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

In addition, 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, security teams 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 across all applications, operating systems and devices to reveal the fundamental actions of attackers in network traffic, even encrypted traffic.

Artificial intelligence that leverages data science, machine learning and behavioral analysis is needed to identify and monitor hidden tunnels, data leaving the environment, malware receiving C&C instructions, outside attackers using remote access tools, and attackers delivering malware updates.

Behavioral analysis can quickly distinguish between human and machine-driven traffic. This capability can flag an attacker using a remote administration tool by revealing that what appears to be an end-user connection is actually a connection 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.

In the 2016 Vormetric Data Threat Report, a survey of more than 1,100 senior security executives from across the globe, 57% of respondents cited complexity as the number one barrier to wider adoption of data security tools and techniques.

Lack of staff was the second highest barrier, cited by 38% of respondents. The research goes on to note that "a chronic and growing shortage of skilled security personnel" is a problem across the industry.

The solution

Higher education institutions need a network security solution that reduces the work for overburdened IT staff instead of creating more work. This requires a solution that is comprehensive, easy to deploy, and automates real-time threat detection 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, and focuses staff attention on actual attacks in progress by pinpointing the physical devices at the center of an attack and alerting staff when there is high threat activity.

Cognito detects attacks in progress, streamlines operations

Cognito enables higher education institutions to detect and respond rapidly to threats, before any damage is done. Picking up where perimeter security leaves off, Cognito provides deep, continuous analysis of internal and Internet traffic and detects the fundamental actions and behaviors that attackers must perform when they spy and spread inside the network in search of valuable assets to steal.

Leveraging artificial intelligence that uniquely combines data science, machine learning and behavioral analysis, Cognito 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 threat. This enables security teams to immediately focus on the highest risk detections.

Cognito also learns about the naturally occurring behavior patterns in an organization's network and provides a visual map of the relationship between threats, hosts and key assets such as PII in student records.

With Cognito, higher education institutions can quickly and easily address security, compliance and manpower challenges. For example, Cognito helped Barry University stop an attack in progress when the institution was the victim of a phishing campaign.

As individuals clicked on the malicious emails, IT staff started seeing endpoint protection alerts. Cognito's real-time monitoring revealed a targeted attack in progress, enabling the security operations team to stop the attack, preventing data theft.

Address today's dynamic threat landscape

Cognito 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 applications and operating systems as well as BYOD and IoT devices.

Combining machine learning, data science and behavioral analytics, Cognito detects the attack behaviors of known and never-before-seen threats at any stage across the entire attack surface of an organization. Threat detections are automatically correlated, scored and prioritized so security teams can promptly stop attacks and mitigate their impact.

Cognito is unique in that it uncovers the fundamental behaviors of cyber attacks, 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.

Cognito provides proof of technical controls in multiple fundamental areas

Meet the challenge: Know your business, know your risk

For example, Cognito offers 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 administrator credentials to escalate privileges.
- The ransomware file encryption activity itself.

Because Cognito recognizes patterns of traffic, there's no need to crack open packets to see what's inside, preserving data privacy for encrypted traffic. Cognito 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.

Similarly, Cognito uses data science, packet-level machine learning and behavioral analysis to identify the presence of external remote access, even malicious remote access tools that are customized or unknown to the security industry.

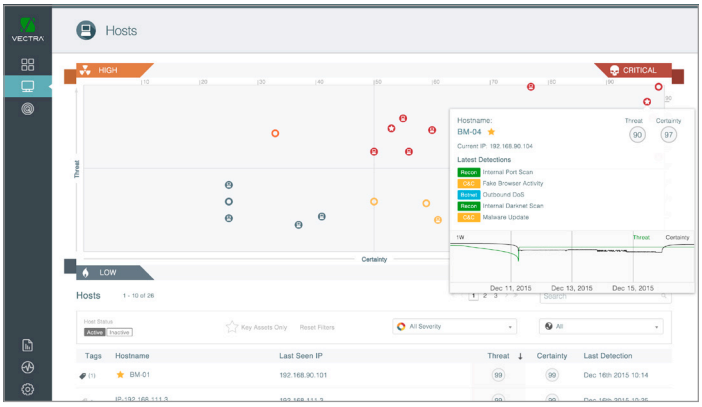
Streamline operations and save staff time

Understanding that the time of security analysts comes at a premium, Cognito is designed to be easy to deploy and use. Automation plays a pivotal role.

Cognito automates the tedious, manual work associated with a Tier 1 security analyst's job and consolidates vast amounts of threat 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 threat investigations and have successfully deferred analysis to IT generalists instead of escalating simple investigations to higher paid experts.

Cognito pinpoints physical hosts at the center of an attack and automatically tracks and scores threats in context over the full duration of the attack. The Vectra Threat Certainty Index displays alerts so security teams instantly know which network hosts with attack indicators pose the biggest risk with the highest degree of certainty.

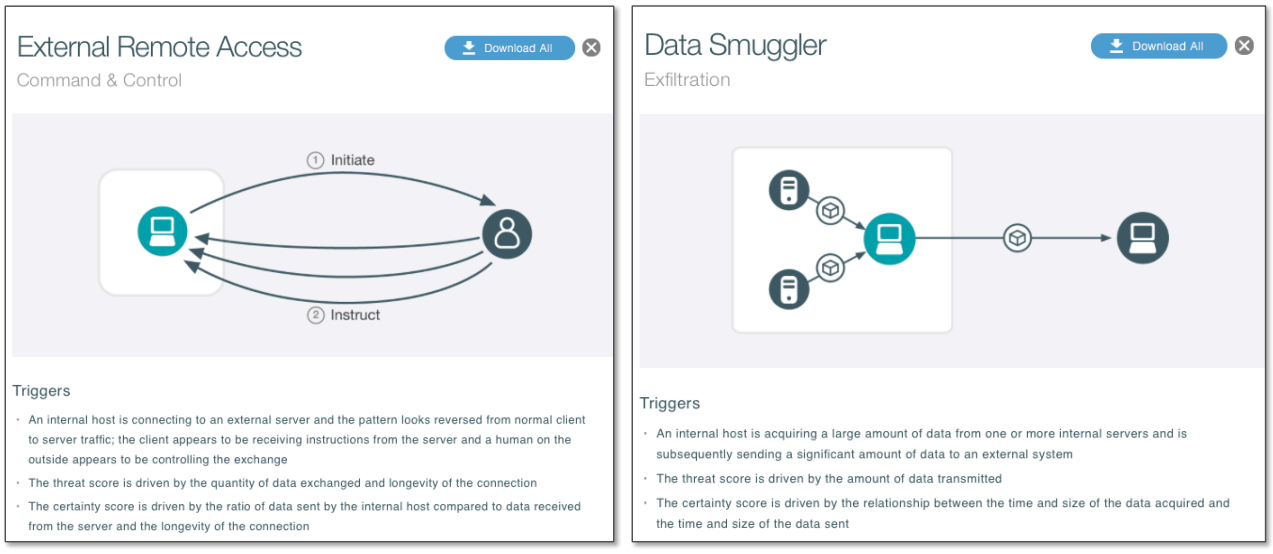


Cognito pinpoints physical hosts at the center of an attack and automatically tracks and scores threats in context over the full duration of the attack

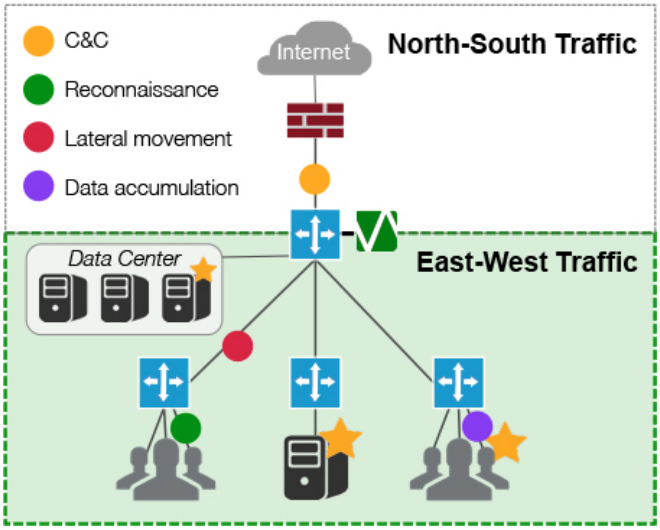
Details about an attack are just one-click away, so staff can easily view metadata from the exact packets between the compromised host and other internal assets it is attacking or external parties with which it is communicating, and respond accordingly.

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

In addition, Cognito 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.



Simple detection explanations: Evidence of technical controls



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

And finally, a robust API allows Cognito 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 pre-correlated Vectra detections and host scores.

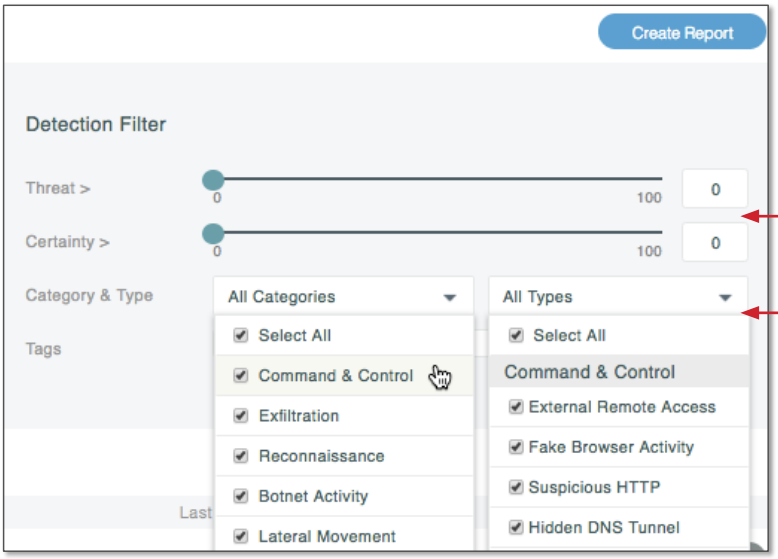
"Vectra's advantage is we get more information about the threats, and data that's automated and actionable," says Bryan McClenahan, senior information security analyst at Santa Clara University. "We don't have 30 to 40 security engineers so we've got to be smart."

Deliver compliance data on demand

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

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

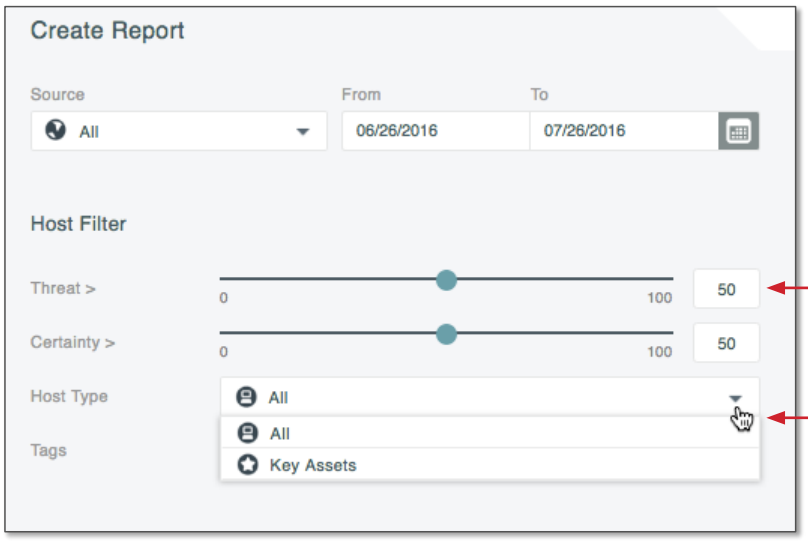


Filter events based on threat to the network

Easily report on controls specific to any phase of attack:

- Malware behavior
- Lateral movement
- Data loss

Easily document controls based on type of threat



Track and document any and all hosts in your network

With Cognito, 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 highlight specific data, such as all hosts with threat certainly scores above 50.

Conclusion

Institutions of higher education will continue to be a top target of cyber attackers. Cognito arms security teams with an automated solution that works in real time to rapidly detect known and unknown cyber attacks inside any network across the constantly evolving threat landscape.

With the unique ability to detect and mitigate network cyber attacks while they are happening, Cognito enables security teams to respond with unprecedented speed, accuracy and efficiency – well before the bad guys can steal sensitive records or critical research.

Likewise, Cognito gives security teams unparalleled network visibility into malicious attack behaviors and automates the hunt for cyber attackers, while at the same time allowing organizations to quickly and easily respond to audits and have more time to concentrate on keeping key assets safe.

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai