cybereason

Resolving Security's Biggest Productivity Killer

How Automated Detection Reduces Alert Fatigue and Cuts Response Time

In today's security environment, organizations realize attackers are likely already inside a company's environment or will find a way to get in no matter how well the organization is protected. As a result, security programs are now more proactive, with analysts actively searching for the hackers that defeated the company's defenses.

Our **ebook**, "The Seven Struggles of Proactive Detection and Response", discusses the challenges security teams face when attempting to proactively hunt for adversaries.

Organizations that manually hunt hackers face time-consuming and inefficient processes. This is where automation is beneficial. Automated cyber hunting was developed to minimize the amount of time security analysts spend building a detection program and eliminating the need to configure alerting tools. The main benefit of adding automation to the detection and response processes is the ability to significantly increase their effectiveness.

The time spent manually investigating alerts and eliminating false positives hinders a security team's ability to protect their organization.

Automated Detection Supplements Security Teams

As organizations adopt a proactive detection approach, larger security departments are building and training in-house hunting teams. However, many organizations are either too small or lack the expertise to run such an operation. Automated detection is helpful in both cases. For larger security teams, it increases productivity and decreases the amount of time spent managing tools. For smaller teams, automated hunting jump starts their ability to proactively hunt for malicious operations.

The Key Features of Automated Detection:

Data collection

Quality detection starts with gathering good data. That means spotting events in real time and continuously collecting data with as much coverage as possible across the entire environment.

Data analysis and cross-correlation

Data interrogation is one of the most time-consuming parts of any analyst's job since the process heavily relies on data mining and query building. Automating these two processes expedites the process of turning raw data into useful information.

Ability to work with various data sources

Traditionally, whenever a new system was added to the work environment, new queries had to be built and added to the correlation list to ensure coverage by the detection engine. Automated systems have the elasticity needed for consuming various data sources, enabling the detection engine to easily scale as the organization grows in size and complexity.

Incorporating threat intelligence

Threat intelligence feeds are commonly used by security teams to learn about new attack vectors. In order to turn them into an actionable detection tool, security teams need to build and constantly update rules and queries to actively search for the existence of malicious evidence. New threat intelligence is published on either a daily or weekly basis, making it almost impossible to manually keep up with the pace of updates. Often, organizations end up ignoring the threat feeds they have subscribed to.

Automated detection approaches streamline this process: they consume threat feeds and automatically cross-correlate them to what appears in a company's environment to find indications of malicious behavior.

> *Recent research reveals that 69% of organizations say that their security tools do not provide enough context for them to understand their risk.*

Behavioral discovery of non-signature based and non-malware based attacks

Without automation, the ability to detect new attacks completely relies on the experience and intuition of seasoned security analysts. Level 3 analysts often talk about a "hunch" as the first indicator that leads to the discovery of a complex hacking operation. But relying on a hunch is risky and can result in many attacks going undetected for more than 200 days. The introduction of machine learning and computational analytics enables the identification of abnormal behaviors without being bound to rigid IOCs (indicators of compromise).

Automated hunting seeks patterns of malicious behavior, rather than a specific hash or signature. This uniquely enables them to spot fileless and malwareless attacks. These attacks use legitimate administrator tools like Windows Management Instrumentation and Powershell, making them extremely hard to detect. In fact, use of these vectors is on the rise.

Eliminating false positives

Alert fatigue is probably the biggest drain on a security teams' productivity. Not only do excessive false positives waste an analyst's time, they also desensitize security teams, making them overlook real malicious activities. The introduction of an automated hunting system provides a faster approach for differentiating between abnormal yet benign activities and truly malicious behaviors. Since hunting machines automatically cross-correlate data across the organization and put things in context, they can distinguish between local, unsubstantiated abnormalities and pieces of evidence that, when combined, clearly fit an attack pattern.

Providing context for response

Automated hunting solutions reduce the need to gather forensics for incident response. This eliminates the need for manual information gathering leading to a faster and effective response.

Validation

Any hunting workflow has to be properly validated to ensure security measures are always current and can detect a wide variety of adversaries. While security teams commonly perform penetration tests on their protection systems to discover vulnerabilities, they rarely test a detection engine since that requires the knowledge and capabilities that only large, very sophisticated teams can afford. Even though organizations invest time, effort and money into building rules into various detection platforms, they rarely test them to check if they're able to spot an attack. Automated hunting solutions can also automate their self testing. Thanks to machine-learning algorithms, the system learns and improves itself when it tries to detect new attack vectors.

The Benefits of Automated Detection

1. Eliminating detection management

One of the most important advantages that an automated system offers is the ability to automate query building and scale the integration of threat intelligence into the detection process. The Cybereason platform, for example, integrates data analytics and pattern recognition to search for an attacker's behaviors without the need of an organization's security teams to build queries or parse data.

2. Enhancing detection and response

Furthermore, when combined with machine learning, the platform detection capabilities evolve to learn from and adapt to a firm's environment, as well as to new threats. This enables organizations to improve detection and response to signature-based threats, and opens the door for the identification of new threats.

3. Addressing deception

Attackers use various deception tactics that humans commonly fail to catch. A sophisticated automated hunting machine can help organizations overcome deception and evasion techniques and are immune to the misconceptions that humans tend to have.

4. Security team empowerment

For most companies, the largest benefit from implementing automated hunting is a significant improvement in security team workflows. This method amplifies collaboration and eliminates geographic and departmental silos.

On an individual level, automated hunting provides direct benefits to security analysts. First, it significantly reduces alert fatigue by eliminating the false positives that add stress and time to everyday work. This is due to machine-learning algorithms' ability to discriminate between abnormal but benign user behavior and malicious activities, and only issue alerts on incidents that truly threaten a company.

Second, it eliminates the need for security personnel to develop parsing rules and correlate data. There's no reward for analysis and cross-correlation. The reward is discovering and stopping the threat. Automation helps reach these goals faster.

5. Leadership visibility and control over the threat landscape

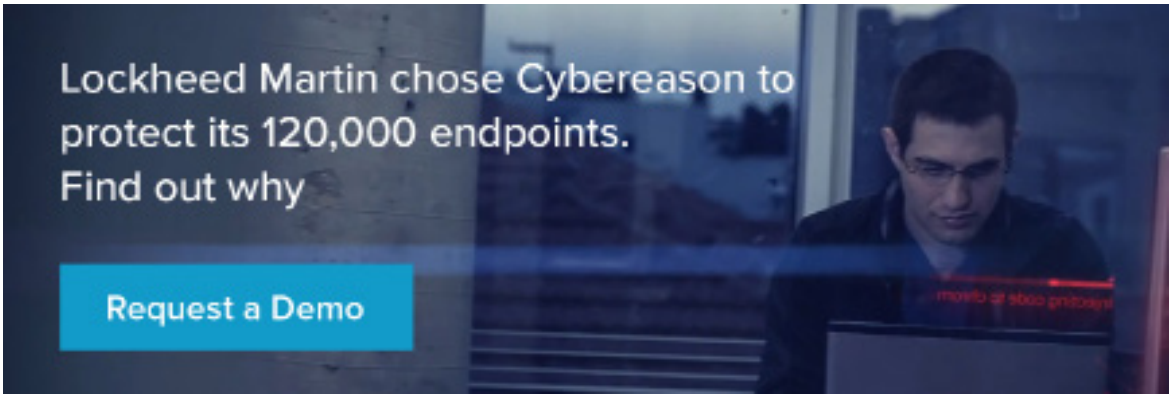
Automated hunting products also provide advantages for a company's leadership, like the ability to offer real-time visibility into an organization's threat landscape.

Additionally, once a breach occurs, a CISO will immediately want to know the event's root cause, timeline and impact. By automating detection and investigation, CISOs can get this information instantaneously without waiting for their technical teams to gather the data from various systems. This helps security executives stay on top of the most recent threats their company faces and ensure their teams are proactively halting them.

The Future of Cyber Security: Speed and Simplicity

As cyber attacks become more sophisticated, automatic detection is vital to keeping companies safe without further burdening overworked security teams. By helping companies know if they're under attack, automated detection allows security teams to proactively respond to threats without using the labor-intensive processes associated with manual hunting.

Automated hunting is the key to returning power to the defenders. A platform that can reveal hacking operations as they unfold is the innovation the security industry needs.



cybereason

Cybereason was founded in 2012 by a team of ex-military cybersecurity experts to revolutionize detection and response to cyber attacks. The Cybereason Malop Hunting Engine identifies signature and non-signature based attacks using big data, behavioral analytics, and machine learning. The Incident Response console provides security teams with an at-your-fingertip view of the complete attack story, including the attack's timeline, root cause, adversarial activity and tools, inbound and outbound communication used by the hackers, as well as affected endpoints and users. This eliminates the need for manual investigation and radically reduces response time for security teams. The platform is available as an on premise solution or a cloud-based service. Cybereason is privately held and headquartered in Boston, MA with offices in Tel Aviv, Israel.