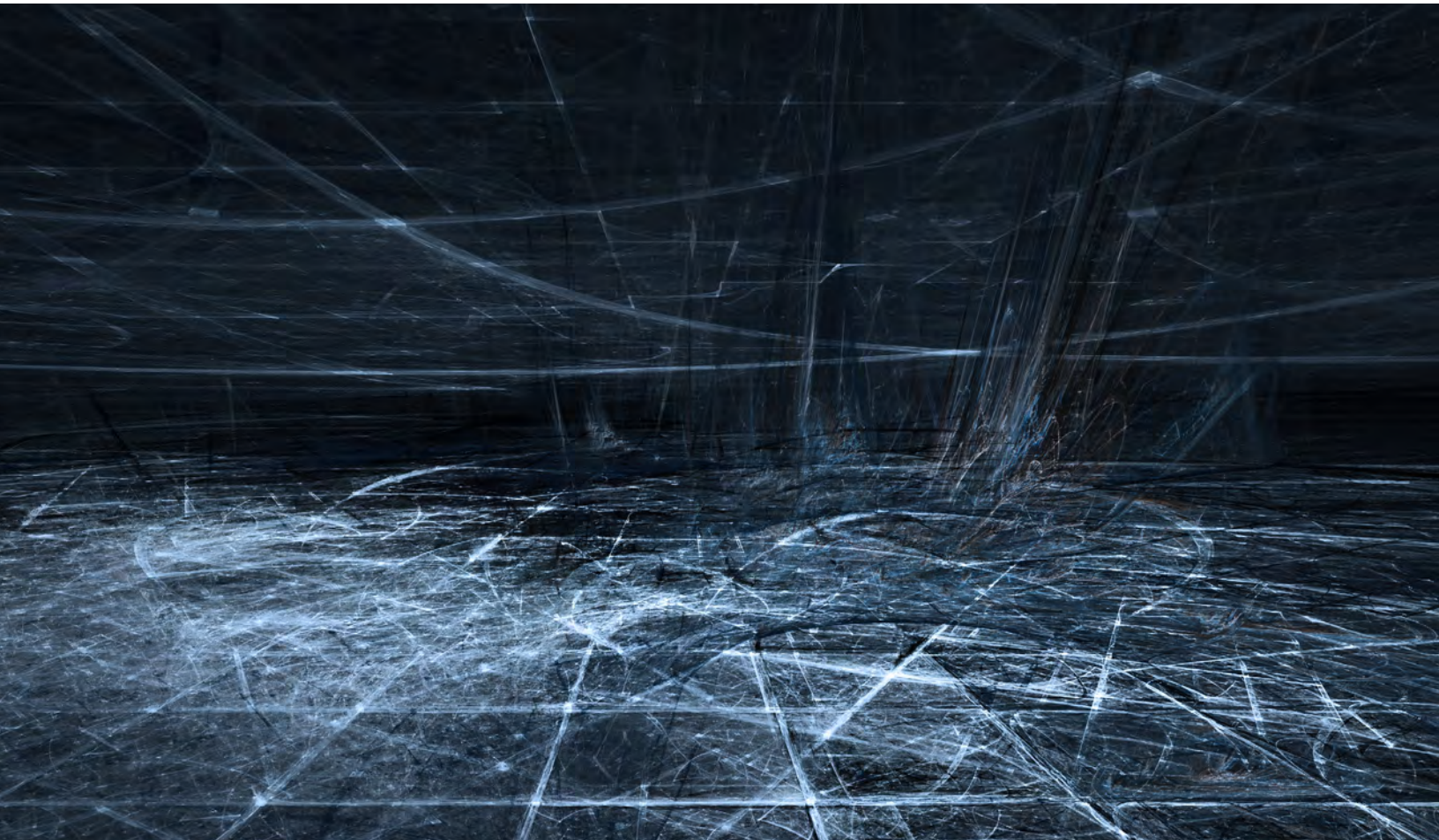
cybereason

The Seven Struggles of Detection & Response

How Manual Detection Hinders Security Productivity



Introduction: A Shift to Proactive Cyber Defense

A string of high-profile data breaches has proven that even the most heavily fortified companies are vulnerable to motivated attackers.

Organizations need to accept they'll eventually get breached and, in fact, their environment may already be compromised. This new threat landscape requires adding cyber detection to an organization's security strategy. Proactive detection, also known as cyber hunting, closes the gaps that traditional security tools, such as firewalls, antivirus software and sandboxes, neglect.

Hunting for adversaries results in cyber attacks being detected earlier in their lifecycle, potentially limiting the amount of damage a breach can cause.

This eBook introduces the concept of proactive breach detection and discusses its advantages.

Organizations that attempt to manually hunt adversaries face a time-consuming and inefficient process.

Manual Hunting: Mission Impossible?

Organizations that attempt to manually hunt adversaries face a time-consuming and inefficient process. Typically, this method entails security teams gathering, sorting and analyzing all of the relevant data a company creates in as close to real time as possible.

Large businesses tend to set up security operation centers that handle tasks including manually hunting for adversaries. But manual hunting is challenging, even for companies with deep pockets and large security teams. In many cases, security staff simply lack the knowledge necessary to deal with the complex attacks they're facing.

Adversaries are now using tactics that extend beyond basic malware. These next-generation attacks are designed to burrow deep into a network and persist even after a breach is detected and the attack is supposedly shut down.

Meanwhile, small companies often forgo manual hunting since the process is labor intensive and they lack the staff with the necessary skill set.

The seven most common limitations to human-based cyber-hunting approaches are:

1. Chasing Indicators of Compromise

The most common approach for detecting attacks entails looking for indicators of compromise. Common IOCs include virus signatures, malignant IP addresses, MD5 hashes of malware files and URLs or domain names linked to botnet command and control servers. If any of these are observed on either a network or operating system, a breach has most likely occurred.

While basic IOC updates such as signatures and hashes can be routinely fed into an antivirus platform, others require manually building parsing rules into various systems in order to detect an indicator and issue an alert. This leads to organizations constantly trying to catch up with their adversaries. A company's detection capabilities are only as good as its ability to build IOC-based alerting mechanisms.

"It can easily take me an hour to write one simple parsing rule in our SIEM," a senior security architect in a large pharmaceutical company recently told Cybereason. "Only to find out two weeks later that one of the folks in IT

changed the configuration of the firewall, breaking the rule and making me re-do the whole work to make the rule operational again. In order to cover our entire international organization we have to maintain over 5,000 rules."

IOC management has clearly become security's Sisyphean task.

2. Attackers Use Deceptive Tactics to Avoid Getting Caught

Even if analysts are able to build a system that's robust enough to access, gather and query all of the necessary information to protect their environment, they need to consider that hackers may use deception to evade detection. Hackers are aware of common IOCs built into a company's detection systems and constantly adapt their strategies to deceive them. To stay ahead of the adversary, organizations have to use more sophisticated, dynamic tactics that keep evasion and deception techniques in mind.

Hackers can utilize a variety of exploits and vulnerabilities to attack an organization, giving security analysts a substantial amount of data to collect and analyze.

3. The Knowledge Limitation

One major issue security analysts face is tracking a seemingly endless number of possible attack vectors. Hackers can utilize a variety of exploits and vulnerabilities to attack an organization, giving security analysts a substantial amount of data to collect and analyze.

In fact, according to the **Verizon Data Breach Investigation Report,** between 70 percent and 90 percent of malware samples are unique to an organization, showing that firms must track a variety of malware and attack vectors. Analysts also need to stay abreast of the latest threat intelligence and constantly compare gathered data against known attack information.

By far the most challenging aspect of their job is handling new, targeted attack vectors. Identifying them requires experienced staff who can intuitively spot abnormal behavior and manually check incidents to see if they're either malicious or benign. This is a tedious process that doesn't scale easily.

4. Operating in a Complex Environment - The Visibility Gap

Manual hunting becomes even more difficult when factoring in that analysts need to gather all of this data across a complex and fragmented enterprise.

Often, SOCs have blind spots due to an organization running multiple isolated networks, an inability to collect real-time information from some endpoints and the complexities of operating in multiple geographic locations, among other issues.

5. The Response Time Challenge

The multiple steps involved in manual detection slow down threat response time. Manual detection usually entails a security professional first receiving an alert about malicious behavior, and quickly determining if it's legitimate. Next, the analyst figures out what caused the alert and understands its implications before finally taking action.

However, even in SOCs that are staffed with highly skilled analysts, gathering context on an alert and making a decision for an appropriate action takes hours or sometimes days. Manual hunting calls for long investigation times, which only adds to the scalability problem.

6. The Challenge of Validation

Even the most sophisticated, proactive hunting teams often lack an adequate plan for testing their detection capabilities. After security teams build queries and closely observe their environment, they need to validate their ability to spot hacker's activities. This goes beyond traditional penetration testing, which mainly focuses on vulnerabilities that lead to the network being compromised.

7. Alert Fatigue

IOC-based detection approaches, which are rigid and look for a finite yes/no answer, have a tendency to produce either an excessive amount of false positives, or high false negative rates, depending on the threshold set into the system. False alerts can desensitize security teams, causing them to tune out these notifications and place an organization at risk.

This could have happened in the Target breach. The retailer's malware solution detected the program that was used in the attack, but Target's security team supposedly ignored the alerts. They claimed to receive hundred of alerts every day and had difficulty determining which threat was especially malignant. There's a dire need for an approach that prioritizes alerts on the most malicious activities.

Automation comes to the rescue

Companies need to adopt a proactive cyber-hunting approach as they shift to to a post-breach mentality.

Building and training an in-house hunting team requires highly talented security analysts and is also extremely inefficient and ineffective. New automated cyber-hunting technologies that use machine learning and big-data analytics address these issues.

Cybereason's platform automates cyber hunting, detecting cyber attacks in real time and cutting incident response time from weeks to hours.

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.