ONE-TOUCH THREAT MITIGATION

This component of the Anti-SIEM focuses on mitigating advanced threat attacks easily.

In this document, we'll focus specifically on the mitigation capabilities of Cyphort's one-touch threat mitigation, the layer that enables Anti-SIEM users to effectively mitigate threats in their environment.

How one-touch threat mitigation solves detection and incident response problems

Most enterprises rely on in-line security devices to block advanced threats. However, in-line security devices can only carry out signature-based detections. This is because they need to process a lot of traffic in a short amount of time, and as a result, performance takes priority over prevention. Advanced threats contain completely new malware samples that evade signature-based detection. Their payloads must be analyzed based on behavior rather than rules or signatures. Although it may seem that this approach requires more processing compared to signature-based detection, this is the best way to detect unknown threats. So rather than trying to "prevent" advanced attacks, the focus is on detecting and mitigating threats as early as possible. The Anti-SIEM accomplishes this using a combination of behavioral analysis and machine learning technologies for fast threat detection.

Once the threats are detected, there are two important mitigation steps that must be taken:

- **Isolation of an infected endpoint** through coordinated response with NAC or endpoint tools
- **Configuration of prevention rules** on in-line security devices to strengthen them and help prevent similar attacks in the futures

Enterprises often invest in multiple best-of-breed products for various security operations, so it can be difficult to easily mitigate without integration between devices.

To solve these problems, the Anti-SIEM was designed to:

- **Detect advanced threats** across all vectors
- **Integrate with other devices** in the customer's environment to collect contextual information and evidence
- **Leverage existing security infrastructure** to mitigate threats with ease

One-Touch Mitigation Highlights

Cyphort's Anti-SIEM includes one-touch mitigation of advanced threats at all stages of the cyber kill chain. One-touch mitigation provides customers the ability to integrate with other security devices and automatically mitigate threats instead of having to manually interface and update each security device with new rules. Customers also have the option to use a hybrid mitigation

The Anti-SIEM from Cyphort delivers three key values:

Advanced Threat Detection
Advanced Threat Analytics
One-Touch Threat Mitigation

Benefits

The Anti-SIEM's one-touch threat mitigation offers the following benefits:

- **Leverages the existing security infrastructure to block advanced threats.** Traditional security devices in the customer's environment can be utilized to block unknown threats detected by Cyphort. This flexibility helps maximize the value of customers' existing investments, saving time, money and effort.
- **Mitigation of threats across all stages in the kill chain.** Response to a threat can vary based on threat progression. It's important to effectively mitigate the attack, prevent the spread of the attack, and prevent future attacks.
- **Proactive blocking.** Patient Zeros can be avoided by proactively protecting the enterprise against suspected malicious websites, servers and malware campaigns.

approach which gives them the flexibility to first review and approve changes before any new rules are automatically pushed to devices.

The following are examples of mitigation approaches to threat vectors:

- **Email.** This continues as the primary vector for delivering advanced malware. As enterprises host email in the cloud, they become more vulnerable. Cyphort provides the ability to automatically quarantine emails on Google and Office 365 using REST APIs. This prevents the malicious emails from getting delivered to the user's mailbox in the first place.
- **URLs.** When malware gets downloaded over the network, the malicious URL is pushed to secure web gateways to block endpoints from further accessing the URL. Similarly, communications between the infected endpoint and the command and control servers are blocked by pushing malicious IP addresses to firewall devices.
- **Infected hosts.** These are isolated through integrations with network access control devices and endpoint detection and response solutions.

Quilt Technology Partners

Partners in Cyphort's Quilt Security Ecosystem leverage open APIs to integrate with the Anti-SIEM. Cyphort integrates with vendors such as Cisco, Fortinet, Juniper, Bluecoat, Check Point, Palo Alto Networks, Carbon Black and Bradford, among others. Partnerships span three categories: network, endpoint, and infrastructure. For more information about Quilt, please see our Technology Partner page available on the Cyphort website.

Cyphort Labs

Cyphort also offers proactive mitigation, which is a compiled list of malicious URLs and IP addresses curated by the malware research team. This list is created based on research and malware trends seen in the wild.

Conclusion

Cyphort's one-touch threat mitigation empowers the incident response team to remediate advanced threats effectively and easily for email, web, and lateral spread traffic in your network.

To understand more about the Anti-SIEM, all of its components and features, and its value to your organization, be sure to visit the resources section on the website. To arrange a demonstration, please call us at 1-408-841-4665 or email info@cyphort.com.

About Cyphort

Cyphort is a privately held cybersecurity company founded in 2011 and based in Santa Clara, CA. The company provides SMB and enterprise customers with the Anti-SIEM, an open, scalable software platform that combines advanced threat detection, analytics, and mitigation capabilities. The solution minimizes the cost and complexity of traditional SIEMs, while delivering immediate, actionable insight into security incidents for fast threat resolution. www.cyphort.com.

CYPHORT

5451 Great America Pkwy, Suite 225, Santa Clara, CA 95054 | P 1.408.841.4665 | F 1.408.540.1299 | info@cyphort.com
Sales/Customer Support P 1.855.862.5927 | F 1.408.540.1299 | support@cyphort.com