SOLUTION BRIEF

The Open Architecture of the Anti-SIEM

Leverage Advanced Intelligence and Your Existing Workflows and Systems

The Anti-SIEM from Cyphort combines advanced threat detection, advanced threat analytics, and one-touch threat mitigation to empower security teams to quickly identify and resolve security incidents in their network. Just as importantly, the solution leverages open APIs that enable seamless integration with your existing security ecosystem, so your organization can optimize protection throughout the network. This document offers a look at the solution's open APIs and shows how you can use them to strengthen security and improve staff productivity.

Introduction: Security Challenges and Requirements

Challenges

Despite massive security investments, devastating cyber attacks continue to plague enterprises and government agencies. Fundamentally, the issue is that security teams lack the advanced intelligence they need when they need it. Too often, they found out about breaches after the fact. Further, when they do find out about attacks, they lack the insights they need to address the threat most effectively, contain its spread, and mitigate its damage. Some of the most common obstacles are:

- **Isolated visibility.** What visibility security teams do have tends to be isolated in nature, so it's hard for a single individual to track threats across multiple systems and environments. Lacking attack context, it is difficult to determine how a threat may have been initiated, the path it took to enter the corporate network, and whether the attack has spread to other endpoints.
- **Limited correlation.** Security teams lack solutions that correlate intelligence across multiple threat vectors, such as endpoints, web, and email. They may have web monitoring capabilities that detect when a user accesses a compromised web page, but they won't know that links to that page were distributed in an email, nor how many other people may have received emails with the same link.
- **Limited automation.** Compounding matters even further is that many security teams are contending with a severe shortage of skills and resources, prompting the need to establish more effective and broad-based automation. Here too, isolated data collection poses significant limitations. For example, a web proxy may detect a threat, and generate a service request in a ticketing or help desk system. While these requests may be generated automatically, ultimately, they will lack structured, actionable metadata for such aspects as the type of detection, the severity of the threat, the IP address of the compromised endpoint, and so on. As a result, staff members don't get the insights needed for fast, effective response, and instead, must resort to manual research and intervention.

Requirements

Today, security teams need innovative solutions that enable detection and fast mitigation of advanced, evasive attacks, whether those attacks are already moving inside networks or about to enter networks. They need solutions that offer seamless integration, and that enable their organization to leverage all the investments that have already been made, including in existing staff, workflows, dashboards, and systems. They need to be able to leverage the intelligence gathered and effectively use it to enhance the protections delivered by systems from multiple vendors. Further, given the severity of skills gaps and staffing shortages in many security teams, it's imperative to automate and accelerate operational tasks. To achieve these objectives, open and easy-to-use APIs are an imperative.

Quilt Security Vendor Ecosystem: Featured Products

Leveraging the solution's open architecture, Cyphort has established built-in integrations with the following products:

- **Network security devices**, including Blue Coat Secure Web Gateways, Check Point Next-generation Firewalls, Cisco Adaptive Security Appliances (ASA), Fortinet FortiGate Next-generation Firewalls, Juniper Firewalls, and Palo Alto Networks Next-generation Firewalls.
- **Endpoint security systems**, such as the Carbon Black Cb Endpoint Security Platform and the CrowdStrike Falcon Platform.
- **SIEM platforms**, including Splunk and IBM QRadar.

Please note, this is a partial list. Cyphort is continually adding partners to its Quilt Security Ecosystem, so if you're interested in support for a vendor that's not listed here, please contact us.

Through open APIs, organizations can maximize the value and efficacy of existing security investments, and establish more holistic security across the organization.

The Power of an Open, Integrated Security Fabric

The Adaptive Detection Fabric (the advanced threat detection capabilities within the Anti-SIEM) offers advanced machine learning and behavioral analysis capabilities that enable security teams to quickly detect and respond to advanced threats that have penetrated their internal network. The fabric features SmartCore, a patent-pending technology that provides continuous, multi-stage analysis of web, email, and lateral spread traffic moving through the network.

APIs Part of Quilt Security Ecosystem

In building the Anti-SIEM, Cyphort was committed to establishing a completely open API architecture. To maximize the value of the solution's open APIs, Cyphort has created the Quilt Security Ecosystem, a partner program that facilitates interoperability with solutions from third-party vendors. The program now includes more than 30 leading security vendors and a broad range of technologies, including next-generation firewalls, secure web gateways, intrusion prevention systems (IPS), intrusion detection systems (IDS), next-generation endpoint security software, security information and event management (SIEM) tools, cloud access security brokers (CASBs), and more.

APIs Maximize the Value of Cyphort's Extensive Threat Information

Through APIs, the Anti-SIEM's detection fabric can aggregate and fully leverage data gathered across the security environment, collecting rich metadata and feeding it into SmartCore. Further, all the intelligence generated by SmartCore is accessible via a REST API. This ensures virtually all existing security solutions can interoperate with the Anti-SIEM.

In the process of detecting advanced threats, Cyphort collects detailed intelligence:

- The solution specifies the IP addresses and URLs that are the source of threats, and that are the recipients of malicious traffic.
- It provides details on the changes an attack makes on the endpoint, including registry keys created, processes spawned, and mutexes (mutual exclusion objects) that have been developed.

All these details give insight into the progress of an attack across the cyber kill chain and help security analysts quickly ascertain where an attack started and how far it's spread. This intelligence can be employed to create custom signatures, rules, and policies for IPSs, secure web gateways, and firewalls.

Key API features

The API offers the following features:

- **Core solution component.** Historically, many vendors have treated APIs as an afterthought, only incorporating them later in the product's evolution, in response to user demand. In contrast, Cyphort developed the Anti-SIEM with an open architecture from the beginning. Cyphort understands how critical APIs are, and treats them as an integral part of a holistic security solution.
- **Long-term solution flexibility and agility.** Moving forward, the solution's open APIs will enable Cyphort to quickly add support for other products and services, helping ensure that the solution keeps pace with changing technologies and customer requirements.
- **Easy to leverage.** The public API used by the Anti-SIEM is easy for customers and partners to leverage. The API is well documented, with extensive examples and straightforward documentation. Through the Cyphort Support Center, customers can also gain access to extensive collections of sample code.

Integration Use Cases

The open APIs are leveraged in two fundamental ways:

- Third-party systems can use an established API account and a key to poll the Anti-SIEM and pull data from it. Through this approach, analysts can inspect logs to identify threats and pursue mitigation efforts.
- Via APIs, the Anti-SIEM can push information to third-party products. To do so, a login for that product is established within the user interface. (See the sidebar for a sample list of currently supported products.) Through this approach, in-line systems like firewalls can automatically be updated, for example, to capture intelligence needed to spot new threats.

By leveraging these capabilities, customers and partners can use the solution and intelligence in several different ways. Following are several common use cases.

Automated Updating of In-line Prevention Systems

The API enables you to establish deep integration with inline detection systems, including gateways, IDS, firewalls, and more. Through this integration, when the detection fabric within the Anti-SIEM finds a new threat, it can automatically provide detailed intelligence directly to the in-line devices, so policies on these systems can be updated to detect or block the new threat.

Cyphort can log in to any supported platform and push threat data, including malicious IPs and URLs discovered. The detection fabric can identify hashes of malicious code, and endpoint systems can leverage these hashes to block access to compromised systems and URLs.

Incident Response

When the Anti-SIEM detects a threat, you can instantly use the detection to trigger an incident response workflow. Threat detection often means that the attack was able to circumvent a number of in-line security systems. Cyphort can detect malware through the behavior it exhibits, or indicators of compromise. It can then capture these indicators of compromise and share these findings with other systems in the incident response workflow, which can provide invaluable insights that help your staff quickly determine the location and scope of the issue.

Intelligence from the Anti-SIEM can be shared with an endpoint security tool, so these systems can determine whether malware was executed on any machines, how many machines have the same file, and so on. As a result, security teams can quickly determine whether an attack is isolated or has spread laterally within the organization.

Intelligence can be viewed in the Cyphort Anti-SIEM management application, which consolidates threat intelligence with related events from other security devices, then presents a complete timeline view of the security incident. Alternatively, the Anti-SIEM can work in conjunction with existing SIEM platforms. In the latter case, security team members can continue to work with their existing workflows and their preferred systems' interfaces and dashboards. At the same time, they can leverage Cyphort intelligence, which enables faster, more effective threat detection and incident response.

Network Access

The Anti-SIEM components can be integrated with systems that manage network access policies, so you can isolate infected elements and keep malware from spreading. For example, if an infected file is detected on a user laptop, controls can be employed to ensure the laptop can't be used to access other laptops or servers. It can be integrated with network access control (NAC) systems and CASB platforms. Following are more details on the integrations of each:

- **NAC systems.** Intelligence can be shared with NAC systems to create prevention rules or prioritize responses to machines. NAC systems can continuously poll the Cyphort platform or receive automated alert logs from the Anti-SIEM. When it detects malware residing on or being transmitted to an endpoint, the NAC can implement a policy-based action in response. In addition, users themselves can be denied access to the entire network or sensitive network domains.
- **CASB platforms.** CASBs can institute policies so that potentially malicious files in incoming or outgoing web traffic can be routed to the Anti-SIEM for inspection. In addition, its threat intelligence can be submitted to CASBs to help inform prevention policies, so, for example, a malicious file can be blocked from being emailed, downloaded, or opened by users.

Benefits

With the Anti-SIEM and its open architecture, your organization can significantly enhance security, while fully leveraging your existing investments in staff, workflows, and systems. Here's how your organization can benefit from its deployment:

- **Enhance security.** It helps you start detecting the stealthy attacks that your first-line of defense has been missing. When threats do arise, it's consolidated timeline view of a security incident can help your team respond with optimal speed and efficiency. By delivering automated feeds of the intelligence gathered, it helps strengthen the security of your existing in-line defenses providing maximum protection for your organization.
- **Enhance operational and cost efficiency.** By integrating the solution with your existing systems and workflows, your team can more fully leverage its existing investments. You don't have to hire more staff, or invest a lot of time in developing new workflows and processes and then training staff how to use them. Further, the Anti-SIEM supports increased automation of incident response workflows, which can reduce operating costs and boost your security staff's efficacy and productivity.
- **Enhance flexibility.** It gives you the optimal flexibility to establish automated workflows and integrations, so you can continue to adapt as your technologies, threats, and processes evolve over time.

Conclusion

With the Anti-SIEM, your security teams can get the invaluable security intelligence it needs to block advanced attacks. Further, the solution delivers the open APIs that enable you to maximize the value of this intelligence across your existing security ecosystem. The result is that you can fully leverage your existing investments and realize significant improvements in your overall security posture.

To understand more about the Anti-SIEM, its open API features, and their 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