USE CASE

Advanced Threat Analytics for Insight into Compromised Users and Endpoints

Executive Summary

For too many security teams, combatting cyber attacks is only part of the battle. Exacerbating matters is the fact that they have to battle against their current tools and the limited context they provide. This use case shows how, with the Cyphort Adaptive Detection Fabric (ADF) solution, organizations can bring together the distributed security intelligence within their networks to gain a unified, contextual view and timeline of all activities related to advanced attacks on users and endpoint devices.

The Demand for Unified Visibility and Context

Companies of all sizes with all levels of experienced staff seek to guard against cyber attacks, but their security teams are wrestling with a significant problem. Fundamentally, staff members lack a comprehensive view of threat activities. While many organizations have implemented security information and event management (SIEM) platforms, the lack of unified threat context limits the effectiveness of operational intelligence to respond to threats quickly.

Customer Problem

Organizations are investing significant amounts of time in manually collecting, aggregating, and correlating data from different tools and resources. When threats are detected, teams are forced to scramble to get answers to critical questions:

- Which host is affected, and who's the user of the system?
- Has the user been targeted previously? If so, when?
- Did our in-line defenses detect the attack?
- Were any traces of the malware left on the system after remediation?
- Has the malware spread to other hosts?

Not only do security teams need to dedicate a lot of time and effort to these manual activities, but the lack of threat context and prioritization of alerts raises other challenges.

- **Significant expertise required.** First-line responders can't easily gain a holistic view of threat intelligence with all the context they need to assess threats and respond. As a result, they have to forward a lot of issues to more senior, second-line responders to get help with investigation and remediation.
- **Increased staffing requirements.** According to a recent Ponemon Institute survey, 69 percent either strongly agreed or agreed with the statement that "We need additional staff to optimize our ability to analyze and respond to data from our SIEM." Also, 61 percent strongly agreed or agreed that they need a better understanding of the context associated with SIEM events.[1]

Massive volumes of alerts from different sources exacerbates the problem. Sifting through duplicate and erroneous alarms can present a significant time drain, and create a lot of noise that makes it more likely that real threats will be missed.

All these challenges result in lengthening the time and increasing the effort it takes to identify and mitigate threats, or more problematically, security teams miss attacks completely.

The Solution: The Cyphort Adaptive Detection Fabric

Cyphort delivers advanced security solutions that enable your organization to establish strong safeguards and address a critical gap in your security defenses. The Cyphort Adaptive Detection Fabric (ADF) solution enables your organization to detect and stop not only modifications of known malware—but entirely new families of malware.

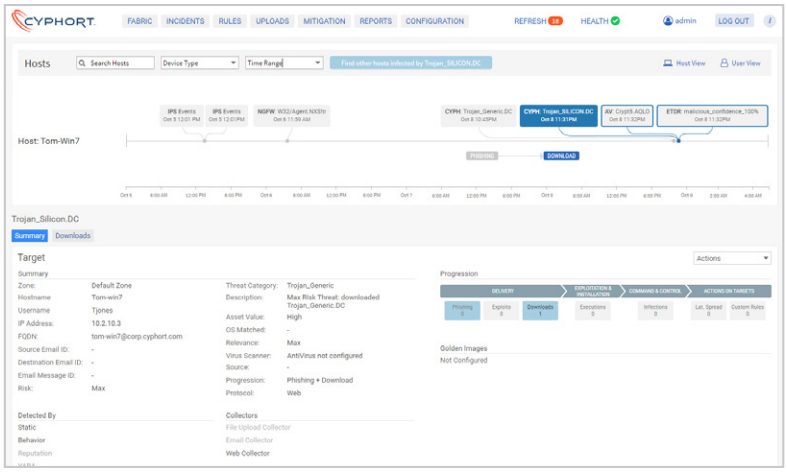
ADF is built with patent-pending technology that provides continuous, multi-stage analysis of Web and email traffic, as well as traffic traversing the network laterally.

ADF continuously collects and correlates data from multiple sources throughout the network, then employs a combination of behavioral analysis plus machine learning to identify virtually all categories of malware. The solution can detect advanced malware and automatically quarantine it to prevent it from causing further damage.

[1] Ponemon Institute "SIEM Technology Report" Larry Ponemon, February 2017

ADF is designed to bring together a holistic view of threat activity from diverse information sources such as Active Directory, endpoint anti-virus, firewalls, secure web gateways, intrusion detection systems, and endpoint detection and response tools. ADF fully automates the collection, correlation, and analysis of logs, events, and alerts.

This complete view of information results in providing response teams with rich data that includes the threat context, the host identity, and the end user identity—with no manual data aggregation and analysis required.



ADF Timeline View

ADF includes a host and user timeline with the evolution and the correlation of advanced threats. With this timeline view, tier-1 teams now have the comprehensive information to determine the exact nature of the threat and whether it's an advanced threat that requires escalation to tier-2 teams for mitigation.

ADF easily integrates with SIEM platforms through its API. Customers can use their SIEM for prioritization and incident handling while leveraging ADF to provide the complete context of advanced threats.

Benefits

When you leverage ADF, your organization can realize the following benefits:

- **Reduce workloads of second-level staff.** ADF delivers the rich contextual intelligence that enables front-line staff to more effectively investigate and remediate incidents, meaning fewer incidents need to get escalated to more experienced second-level staff.
- **Maximize the value of existing investments.** ADF enables your security team to maximize the value of the intelligence captured by your existing security tools.
- **Enhanced staff efficacy and efficiency.** With ADF, your security analysts spend less time sifting through false alarms and get the intelligence they need to spot real threats and prioritize efforts more effectively based on a deeper understanding of events.

Conclusion

With ADF, your security team can get the valuable security intelligence it needs to block advanced attacks and provide context to threats. With ADF, you can gain the rich intelligence you need to address your organization's most critical threats while optimizing operational efficiency.

For an introduction to all of the components and features of ADF, be sure to download the product data sheet.

About Cyphort

Cyphort, Inc. is a network security company providing mid- and large-size enterprise customers with the innovative Adaptive Detection Fabric, a scalable software solution designed to integrate with existing security tools to discover and contain the advanced threats that bypass the first line of security defense in an organization. Based in Santa Clara, California, the company was founded in 2011 and distributes its software through direct sales and channel partners across North America and international markets. Learn more at 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