# ADVANCED THREAT ANALYTICS

This component of the Anti-SIEM improves the productivity of the incident response team by delivering actionable insights into advanced threats.

This document focuses specifically on the capabilities of Cyphort's Advanced Threat Analytics (ATA)—the behavior analysis and machine learning layer that enables Anti-SIEM users to excel at interactive investigations.

## How advanced threat analytics is critical to incident response

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.

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 is 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 must 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 incident context associated with SIEM events.[1]

Massive volumes of alerts from different sources exacerbates the problem. Sifting through duplicate and false alarms can present a significant time drain, and create a lot of noise that makes it more likely that real threats are missed. All these challenges result in lengthening the time and increasing the effort it takes to identify and mitigate threats, or more problematically, causes security teams to miss advanced attacks completely.

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

## The Anti-SIEM from Cyphort delivers three key values:

Advanced Threat Detection
Advanced Threat Analytics
One-Touch Threat Mitigation

## Benefits

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

- **Reduce workloads of second-level staff.** ATA delivers the rich contextual intelligence that enables front-line staff to investigate and remediate incidents more efficiently, meaning fewer incidents need to get escalated to more experienced Tier 2 staff.
- **Maximize the value of existing investments.** ATA enables your security team to maximize the value of the intelligence captured by your existing security tools.
- **Enhanced staff efficacy and efficiency.** With ATA , 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.

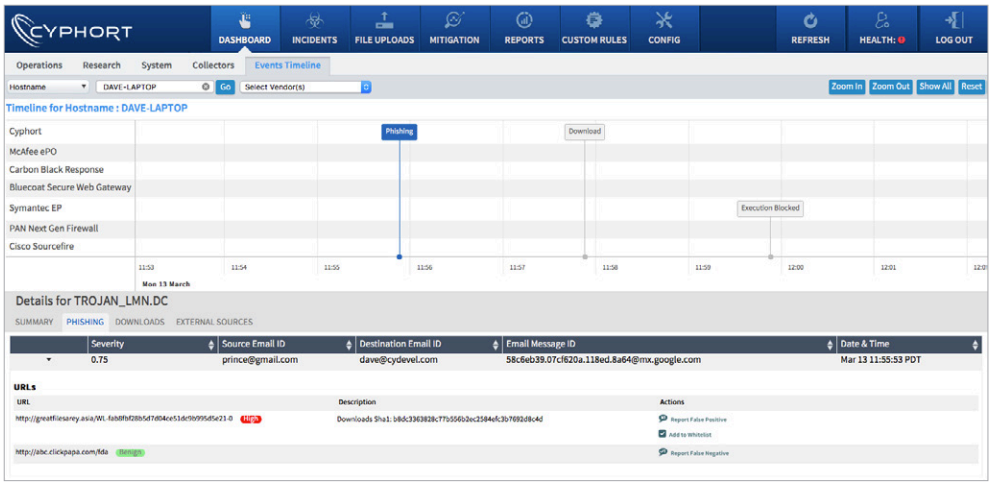
## Advanced Threat Analytics Solution Highlights

Cyphort's advanced threat analytics solution brings 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. Traditional security devices collect valuable information, but most of it goes unused as the devices are not specifically looking for advanced threats. Cyphort's ATA looks at data from different sources, identifies advanced malicious traits and correlates the events to provide complete visibility into the kill chain of a threat. This becomes especially useful in the case of noisy devices such as intrusion prevention systems.

Cyphort's ATA solution is focused around the day to day workflow of Tier 1 and Tier 2 security analysts who work on triaging and investigating malware incidents. A host and user timeline is provided to the security analyst to depict a story about the events that occurred on the host or user. Within minutes, a Tier 1 analyst—who is not a detection expert—can easily determine the course of action necessary for the incident. With ATA, analysts have 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. The Tier 2 analyst is freed up to focus on vetted advanced threats and use the timeline view provided by ATA to perform detailed investigations on the host and user. This holistic 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.

The ATA solution is also very flexible and scalable. It includes an integrated storage architecture that is easily scaled based on the requirements of each customer. For example, some customers only want three months of storage, while others prefer three years of storage to enable deeper historical forensics. The timeline view of security incidents noted above can also be extended to weeks, months, or longer based on the historical data stored by the customer. It can also integrate with existing SIEM solutions. Customers can use their SIEM for prioritization and incident handling while leveraging ATA to provide the complete context of advanced threats.

Customers who don't have a SIEM solution can also benefit because ATA can ingest data directly from other security devices in their network to secure them from cyber attack.




*ATA Timeline View*

## Conclusion

Cyphort's advanced threat analytics empowers the incident response team to effectively identify the most important threats, accelerate investigations and determine effective mitigation.

To understand more about the Anti-SIEM, all of the components and features of SmartCore, 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