opentext™ | Cybersecurity

Position Paper

Enhancing ArcSight Enterprise Security Manager with Threat Intelligence

Implementing MISP as a Low-Volume, High-Context Threat Feed

Stay ahead of the latest cyber threats with up-to-date, easy-to-access intelligence feeds that empower a resilient SOC.

Table of Contents

Introduction

In December 2020, security firms warned that a widely used network monitoring tool, SolarWinds Orion, had been compromised in a malicious cyberattack, putting at least 18,000 organizations at risk. For businesses that used SolarWinds Orion, evaluating and limiting the degree of their organizational exposure in the days and weeks following the discovery of the threat posed significant challenges.

Open-source threat intelligence can provide some critical support in solving this issue. Various communities began sharing information through the Malware Information Sharing Platform (MISP), providing signatures and indicators of compromise (IOCs) within 24 hours of the announced breach. MISP provides a way for organizations to share open-source cyber threat intelligence with the general community, allowing security teams and products to use that intelligence to better detect threats.

The intelligence sharing platform consists of an open-source software tool that can be downloaded, as well as a database of IOCs. This database is used by more than 6,000 organizations worldwide and integrated into a variety of security analytics and threat hunting platforms, including advanced security information and event management (SIEM) platforms, such as ArcSight Enterprise Security Manager (ESM) by OpenText.

A day after news broke of the SolarWinds attack, the Computer Incident Response Center for Luxembourg (CIRCL) released IOCs to its MISP database. Through integration with the CIRCL MISP, ArcSight ESM began evaluating incidents and analyzing data using the new intelligence. SolarWinds-specific threat intelligence included suspicious domains, addresses, URLs, hashes, and even the specific APT groups associated with the IOCs.

The threat intelligence model has also shown its worth during the Coronavirus pandemic, which became a major topic used by cybercriminals as a lure for phishing e-mails capitalizing on COVID concerns, and by nation-state hackers to target businesses and health organizations.

In one case, a phishing e-mail claimed to be sent by a contact-tracing group, informing the user that they were infected. The e-mail urged them to download an Excel form, fill it out, and bring it to the hospital. The file, of course, had malicious scripts that infected the user. The MISP feed caught this activity—and ArcSight ESM labeled it as a suspicious “Macro Embedded in a Coronavirus Spreadsheet”—within 24 hours.

Threat intelligence is a necessary part of any mature security program. Yet, many ArcSight ESM users do not know that they have a ready-to-go threat intelligence feed available to them at no additional cost. This article introduces threat intelligence, highlights the Malware Information Sharing Platform (MISP), and shows how your company can get up and working with the IOCs provided by the database.

Get Intelligent About Detecting Threats

The cyber threat landscape is diverse and massive. In 2020, more than 137 million new variations of malware were detected by companies,[1] nearly 18,400 vulnerabilities were disclosed during the year,[2] and, without security awareness training, 38% of employees were likely to fall for a phishing e-mail.[3]

Adding threat intelligence to your security process can reduce the number of alerts that your security analysts need to triage and speed up your detection of actual threats.[4] Most companies use threat intelligence for detection and response, with indicators of compromise (IOCs) considered as the most valuable threat intelligence, followed by the insight provided into adversary behavior and tactics, according to the SANS Institute's annual *Cyber Threat Intelligence Survey*.[5]

The best threat intelligence feeds curate the most reliable IOCs to create a high-quality source of indicators that can help find malicious activity in a business' environment. Threat intelligence feeds are typically high volume, which—when done poorly—can create an influx of false-positive alerts that can hide malicious activity.

The greatest inhibitors to the effective use of threat intelligence are a lack of trained analysts, as well as a lack of time and funds to pursue threat intelligence, according to the SANS Institute's 2020 *Cyber Threat Intelligence Survey*.[6] All three of these issues can be solved by using the freely available Malware Information Sharing Platform (MISP) with ArcSight ESM's integrations.

The Malware Information Sharing Platform (MISP)
Started almost a decade ago, the MISP open-source threat intelligence platform enables collaboration between organizations researching cyber threats, and sharing of the resulting IOCs through integrations with a variety of security solutions, software, and APIs. The project allows threat data to be collected in a structured format, exported to a variety of intrusion detection systems (IDS), and correlated with the latest information on emerging and previously analyzed threats.

For security analysts that are producing threat intelligence data, the platform allows for sharing of the technical characteristics of malicious activity. The platform also allows for data to be exported to detection systems using a variety of rules and indicator formats—including Snort, Suricata, and Zeek—or the Structured Threat Information Expression (STIX) or OpenIOC format. Perhaps most importantly, MISP helps security analysts avoid duplication of work and provides timely analyses to less technical users who need access to up-to-date intelligence.

For companies that want to consume threat intelligence and use the data in their security program, the rules and threat data—including malicious file hashes, suspicious server addresses, and questionable domains—can be imported on a regular basis.

Exposure Time Reduction
Knowing about the latest threats can reduce a company's cost to clean up the damage from a breach and limit an attacker's ability to do damage. From Winn Schwartau's book Time Based Security, costs are related to exposure time, which is the sum of the time it takes to detect a threat and the time it takes to react or respond to the threat. Reduction of exposure time and risk is a critical function of a security operations team, and is supported by the increased detection capabilities provided through threat intelligence.

1. *Malware: Total Malware chart*. AV-Test. Web page.
2. *National Vulnerability Database: Statistics* Results. National Institute of Standards and Technology. Web page.
3. *Phishing by Industry 2020 Benchmarking Report*. KnowBe4. PDF. 4 April 2020.
4. *What is Threat Intelligence?* Recorded Future. Web page.
5. Lee, Robert M. "2020 SANS Cyber Threat Intelligence (CTI) Survey." Survey. p. 12. 10 February 2020. PDF.
6. Lee, SANS CTI Survey, p. 14.

The Computer Incident Response Center in Luxembourg (CIRCL) leads the development of the platform. The CIRCL MISP threat intelligence database is integrated with a number of cybersecurity products, such as ArcSight ESM, giving businesses a ready source of intelligence. The software and the database of indicators allow security analysts to determine whether they have signs of a current threat within their infrastructure and gives them tools to potentially block further malicious actions.

Overall, MISP has made research easier and more collaborative by offering a free tool that links to large, near real-time threat databases.

Other Intelligence Feeds

The MISP threat intelligence database is not the only source of open-source threat intelligence. Many other threat intelligence feeds exist—some free, others commercial. Feeds such as *Spamhaus* provide a current list to block known spammers and sources of malware. The US Department of Homeland Security's Automated Indicator Sharing (AIS) service shares information about threats reported to the US government's Cybersecurity and Infrastructure Security Agency (CISA).[7]

These are only a couple examples of the many threat intelligence feeds available to SOCs. A few others are listed below:

- Anomali
- EclecticIQ
- LookingGlass
- AlienVault Open Threat Exchange, now part of AT&T
- Emerging Threats, part of Proofpoint
- ThreatConnect
- ThreatGrid, now part of Cisco
- ArcSight Reputation Security Manager Plus (RepSM+) for ArcSight ESM

The Advantage of MISP in Your SIEM

Starting in mid-January 2020, cybercriminals and nation-state attackers began exploiting the Coronavirus pandemic for compelling topics to use as lures for phishing attacks.[8] E-mails written in Japanese claimed that infections had begun appearing in specific parts of the country and urged recipients to check the attached advisory, a document which opened PowerShell in the background and installed the Emotet downloader.[9]

In February 2020, attackers began using Coronavirus-themed e-mails warning about disruptions to global shipping to spread AZORult, an information-stealing trojan.[10] If the recipient opened the accompanying Word document, an exploit for a two-year-old Microsoft Office vulnerability was triggered.

Pre-Emptive Threat Detection

Companies are inundated with security events, often causing alert fatigue for security analysts. Pre-emptive threat detection uses automation, context, and intelligence to prioritize potential security events, reduce alert volume, and allow analysts to respond to true threats fast. Threat intelligence feeds like MISP support these efforts by providing IOCs connected to the latest security threats, which enable SOCs to better detect these threats on Day One and respond to them before damage is done.

7. Cybersecurity and Infrastructure Security Agency. Automated Indicator Sharing. Department of Homeland Security. Web page.
8. Insikt Group. *Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide*. Recorded Future. Blog. 12 Mar 2020.
9. X-Force Exchange. *Coronavirus Goes Cyber With Emotet*. IBM. Web page. 30 Jan 2020
10. Degrippo, Sherod. *Coronavirus-themed Attacks Target Global Shipping Concerns*. Proofpoint. Web page. 10 Feb 2020.

Within 24 hours of both of these incidents, indicators of compromise (IoCs) were available through the MISP threat community.

Initially, these threats were not specifically detected as Coronavirus-themed threats, but as "Suspicious File Hash Activity in Host"—sometimes based on specific hashes *(as in the image below)*,[11] but often based on other data, such as attempts to communicate with a malicious domain.

Using the information, analysts can conduct a variety of additional investigations. More data on the actual files can be called up from VirusTotal, for example, through the ArcSight ESM integration with the malware database. In addition, specific information about the research behind the IOC can be found by clicking through to the MISP instance. Note that the data will often represent research that has not yet been curated in other open-source intelligence feeds, making MISP community instances extremely valuable in catching threats on Day One.

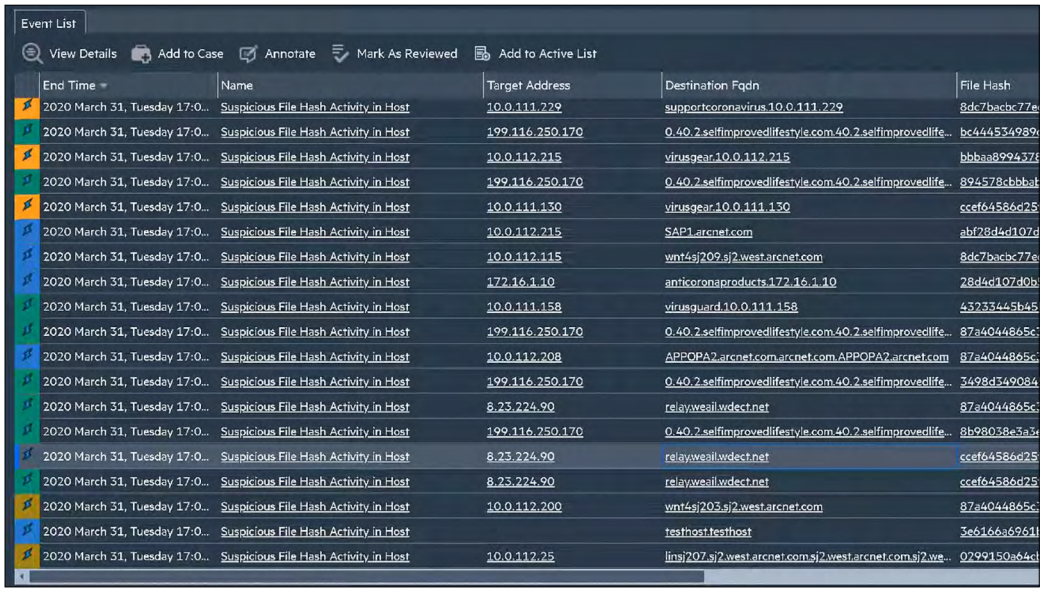

Figure 1. ArcSight ESM Event List with Suspicious File Hash Activity

For more information, see Achieving True Zero-Day Protection with ArcSight ESM, MITRE ATT&CK, and MISP CIRCL.

As specific families of threats become more prevalent, ArcSight ESM will create packages for labeling and alert on specific components of the threat. The Coronavirus (COVID-19) Official Content package,[12] for example, was released for ArcSight ESM on April 14, 2020.

11. ArcSight ESM Unplugged. *Achieving True Zero-Day Protection with ArcSight ESM, MITRE ATT&CK, and MISP CIRCL*. YouTube. Online video. 4 May 2020.
12. **https://marketplace.microfocus.com/arcsight/content/Coronavirus-COVID-19-Official-Content**

In the case of the SolarWinds compromise, companies can use the SolarWinds SUNBURST Detection package, which includes IOCs selected from the MISP data feed, including:

- Dangerous Browsing to a Suspicious SolarWinds URL
- Inbound Traffic from a SolarWinds Suspicious Address
- Inbound Traffic from a SolarWinds Suspicious Domain
- Outbound Traffic to a SolarWinds Suspicious Address
- Outbound Traffic to a SolarWinds Suspicious Domain
- SolarWinds Detected by Vendor

The context provided by threat intelligence can be an enormous aid to researchers, security analysts, and threat hunters, allowing them to reduce their workload and more quickly triage potential security threats. In addition, open-source threat intelligence often provides near-real-time data on threats, reducing the risk to, and the exposure window of, the business. And with easy integration into most SIEMs, adding open-source threat intelligence to your incident-handling process is a no-brainer.

Operational Efficiency

The management of a security operations center is a heavy responsibility, where a complex environment and limited resources can make operational efficiency a truly elusive goal. In order to achieve true cyber resilience, your security team needs a way to be both comprehensive and efficient. The ability to intelligently adapt your resources with automation, a unified platform, and layered analytics can help you optimize the efforts of your SecOps team and achieve operational efficiency.

Three Simple Steps to Get Started

There are a variety of ways to get started with MISP threat intelligence. A security team can download a local instance for the MISP from the project web site and start using the software to help their team collaborate on threat analysis. Alternatively, threat analysts could download an instance of the MISP from one of the analyst communities that support their own instance.

A variety of security products, including the ArcSight ESM Portfolio, will allow you to directly consume indicators of compromise (IOCs) from the MISP community and contribute back to their instances. Here are the steps to get started with MISP in the ArcSight platform's real-time detection and SIEM solution, ArcSight ESM:

Step 1: Get a Key for the MISP Instance

Organizations that want to consume threat intelligence will need to get access to a MISP community instance.

Different communities have different requirements for using their threat intelligence feed. The Forum for Incident Response and Security Teams (FIRST), for example, allows members to use their membership certificate to connect to that organization's MISP instance, while any company can contact CIRCL MISP to join that community.

Step 2: Download and Connect

Once your company has access to an instance, you have to connect the instance to ArcSight ESM.

The Threat Intelligence Platform package must first be imported and installed into ArcSight ESM. While ArcSight ESM versions 7.2 and newer have the package included, older versions of ArcSight ESM will require that the package be downloaded as part of the ESM Default Content from the ArcSight ESM Marketplace.

To import the latest threat intelligence from a given instance, you will need to run the Model Import Connector for MISP on a separate Linux server. The Model Import Connector will keep the list of IoCs up-to-date and consistent. The data imported from the MISP instance includes suspicious addresses, domains, hashes, URLs and e-mails.

For more information, see the presentation Using MISP threat intelligence with ArcSight ESM.

Step 3: Start Investigating

Using ArcSight ESM's Event List view, you can check out the latest events identified using the MISP data. Specific dashboards can be accessed through the Navigator panel for ArcSight ESM, including—for example—the Coronavirus-related Malicious Monitoring dashboard.

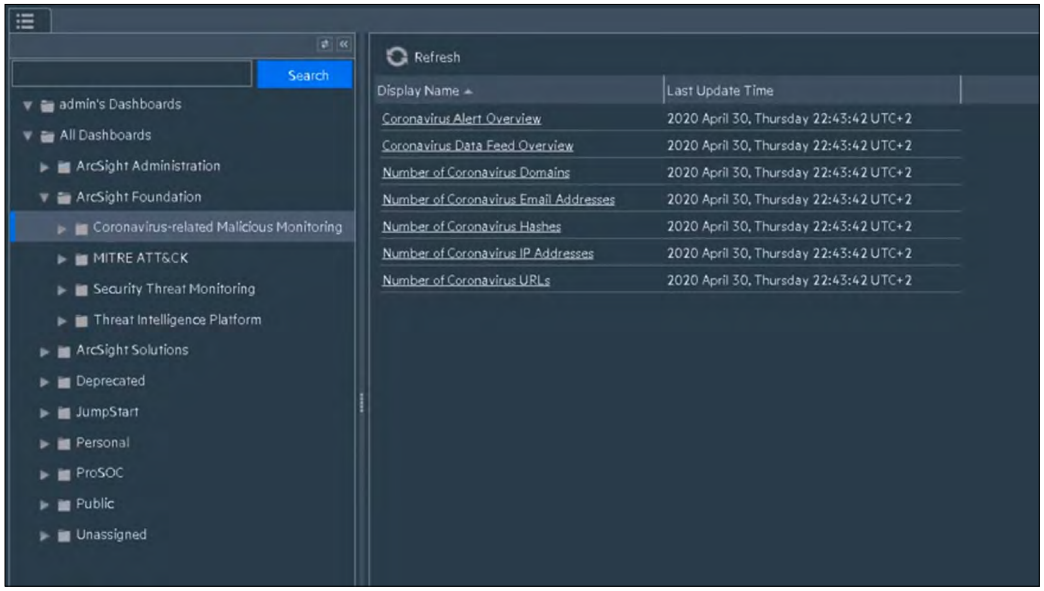

Figure 2. ArcSight ESM's Coronavirus-related Malicious Monitoring Dashboards

Clicking on the Coronavirus Alert Overview will bring up a graphical representation of the data that allows the analyst to drill down on specific alerts based on Rule Name, Attacker, Target and other characteristics.

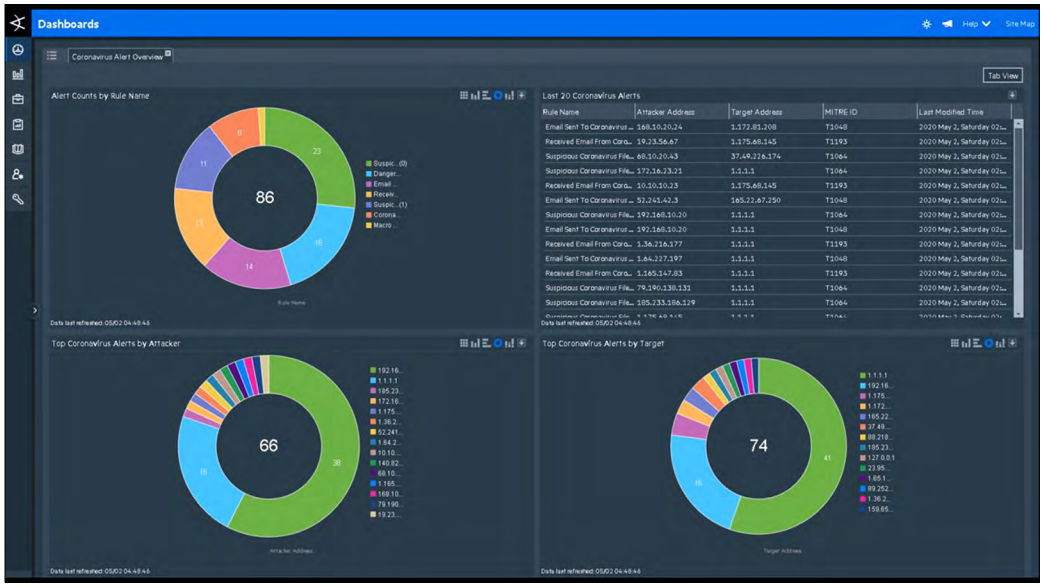

Figure 3. ArcSight ESM's Coronavirus Alert Overview Dashboard

Conclusion

Cyber threat intelligence is a critical part of any cybersecurity operation. The open-source threat intelligence platform MISP lowers the complexity of getting started with using threat intelligence, allowing analysts and companies to quickly get up and running. The platform also supports a robust selection of IOCs that integrate with a variety of cybersecurity products, allowing for automated detection and response to threats.

The platform also gives analysts a great way to learn threat hunting methodology with an incredible ROI. And by enabling collaboration, analysts will not have to repeat a threat analysis that an analyst at another company has already performed. By allowing collaboration across the industry, MISP gives its users a trusted platform through which to share the latest threat information.

Next Steps

For readers interested in learning more about threat intelligence, the Malware Intelligence Sharing Platform (MISP), and ArcSight ESM, here are some useful resources:

- Using MISP Threat Intelligence with ArcSight ESM: Video about getting started with MISP
- Defense-in-Depth Against Coronavirus-themed Cyber Threats with ArcSight ESM: Video about using MISP
- ArcSight ESM Response to SolarWinds Supply Chain Attack: An example of ArcSight ESM's ability to integrate intelligence for rapid response to new threats
- MISP: Software and Tools: A list of modules and APIs that support MISP
- CIRCL MISP Threat Sharing: More information about the CIRCL MISP community

SIEM Correlation Engine in ArcSight Enterprise Security Manager

By correlating events and anomalies in real time, the SIEM Correlation Engine in ArcSight Enterprise Security Manager gives your security operations team more context about events in real time and greater visibility into potential malicious activity. The SIEM Correlation Engine can connect the dots and determine, for example, that malware may try to run because a user has fallen for social engineering. Unlike search-based security event technology, real-time correlation automates the detection of sequences of events to allow for real-time detection of threats.

Connect with Us

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.