Solution Flyer
Security

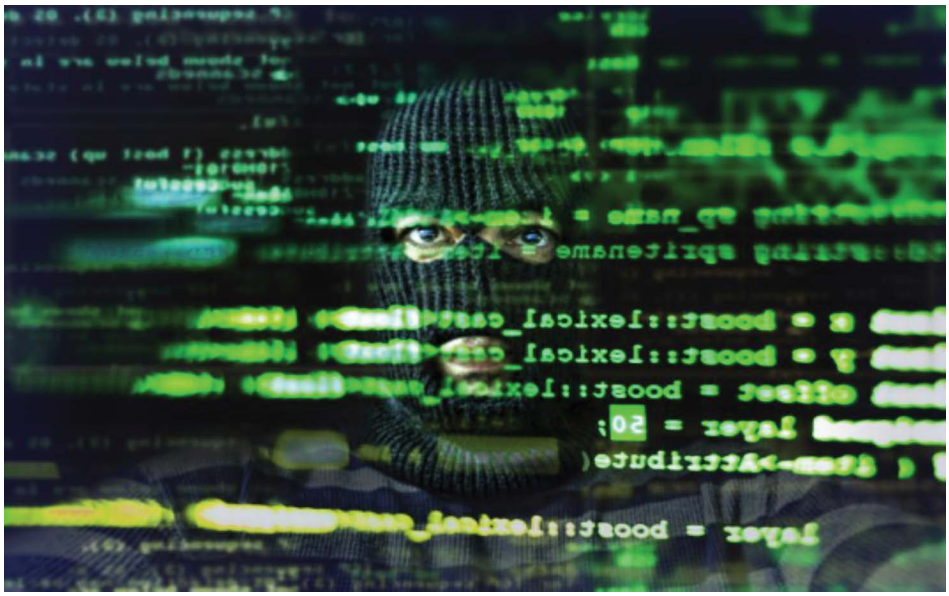
Securing Your Organization: ArcSight and the SolarWinds/SUNBURST Attack

The SolarWinds/SUNBURST attack shocked the world of cyber-security. Many organizations are scrambling to determine the extent of their exposure, and are anxious to know they will be protected against this type of threat in the future.

MITRE ATT&CK Mapping at a Glance:
ArcSight makes it easier for organizations to assess their security posture by incorporating the MITRE ATT&CK Framework into ArcSight ESM and Recon reports and dashboards. Learn how ArcSight's layered analytics work together to protect your organization.

ArcSight and MITRE ATT&CK resources:

+ **Mitre.microfocus.com**
+ Defending against APT groups with Micro Focus & MITRE ATT&CK Navigators
+ MITRE ATT&CK + ArcSight Intelligence (formerly Interset)
+ UEBA and MITRE ATT&CK: Detecting APT-29
+ Achieving True Zero-Day Protection with ArcSight, MITRE ATT&CK, and MISP CIRCL



On December 8th 2020 FireEye announced that they were the victim of a sophisticated cyber-attack[1]. The techniques, discipline and operational security used in the attack lead them to believe it was a state-sponsored attack. As part of the attack, FireEye's elite red-team tools (assessment tools used to test customer security) were stolen. Subsequent investigation pointed to the SolarWinds supply chain system, with complex and targeted methods that experts are referring to as the SUNBURST attack.

On December 12th the CEO of SolarWinds was notified by FireEye of a major security vulnerability in SolarWinds' Orion Software Platform[2]. It appears that SolarWinds unknowingly distributed malicious software through Orion Platform products from March through June of 2020. SolarWinds has since removed the software affected in the attack, and has released hotfix updates to impacted customers. A thorough treatment of the issue is addressed in SolarWinds' Security Advisory FAQ[3], including links to updated software and next steps for the company.

1 **www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html**
2 **https://orangematter.solarwinds.com/2020/12/17/solarwinds-update-on-security-vulnerability/**
3 **www.solarwinds.com/securityadvisory/faq**

The SUNBURST attack and its subsequent media coverage led numerous organizations to reassess their current security protocols. Many are scrambling to determine the full extent of their exposure to this particular threat, and are anxious to know that they will be protected against this type of threat in the future.

ArcSight ESM

Now that the SUNBURST attack has been identified, threat intelligence sources have been updated with specific indicators of compromise (IOCs). ArcSight is committed to keeping your organization secure with the most up-to-date threat intelligence available.

ArcSight ESM users have access to integrations with CIRCL MISP, an open platform threat intelligence service. As soon as exploits were discovered, they were shared on CIRCL MISP. As a result, ArcSight users with the integration were provided with specific, relevant security intelligence as early as **December 14th** to protect their environment. Additional information covering the use of MISP threat intelligence with ArcSight ESM can be found here.

With automated integrations like MITRE ATT&CK and MISP CIRCL, as well as partner integrations with companies like Anomali, Ixia and LookingGlass, your organization can be equipped with the most up-to-date protections available.

SolarWinds SUNBURST Detection Package Features

- Dangerous browsing to suspicious SolarWinds URLs
- Inbound traffic from SolarWinds suspicious address or domain
- Outbound Traffic to SolarWinds suspicious address or domain
- SolarWinds detected by vendor
- T1190-Exploit Public-Facing Application
- T1566.002-Spearphishing Link

ArcSight Intelligence

Some threats, such as insider threats and Advanced Persistent Threats (APTs) are notoriously difficult to detect. These attacks are often complex and avoid detection because they don't have previously defined indicators that are easily spotted. Bad-actors take great pains to behave like other users on the network, but the fact that they are bad-actors means that they will eventually tip their hand.

ArcSight Intelligence is a User and Entity Behavioral Analytics (UEBA) solution that is invaluable in defending against threats like the SUNBURST attack. With behavioral analytics, you don't necessarily need pre-defined IOCs to protect you from malicious activity on your network. ArcSight Intelligence creates baseline "normal" behavior for each entity on your network, and will alert you of suspicious or anomalous behavior specific to that individual. Employees can still have legitimate access to the crown jewels of the company, but it's only when they start filling their pockets that the alarm bells go off.

For illustration, in the case of the SUNBURST attack, the malware downloaded in the Orion Software Package wouldn't set off any alarms on its own. The behavior of the malicious software in the package (compared against the baseline of previous Orion packages) is what would actually be flagged as anomalous. This type of analytics is ideal for defending against zero-day, previously unknown threats.

One of the reasons the SUNBURST attack was so stealthy was because it inserted malicious code into an otherwise trusted software package, distributed from a trusted source. Code development security is especially important for this reason, and that is another area where ArcSight can help. ArcSight Intelligence was built with DevOps in mind, and includes models specifically for code repositories.

ArcSight Intelligence Features

- Baseline behavior for each entity
- Detect anomalous behavior
- Credential access maintained
- Analytics for code repositories

ArcSight Recon

After you've identified a potential threat in your environment, like the SUNBURST attack, you'll want to perform a forensic investigation to determine the extent of the exposure, as well as any damage done. This is where the value of a powerful event log management solution becomes unmistakable.

ArcSight Recon is built for security event logs and is therefore more intuitive and accessible for security analysts, it doesn't require a DBA to operate. It helps hunt and defeat threats by unifying data logs from across organizations, processing billions of events, and quickly making them available for search, visualization and reporting.

ArcSight Recon's columnar database responds to queries faster than traditional databases, enabling it to quickly and efficiently investigate millions of events. Outlier detection provides visualizations to quickly identify deviations from baseline host behavior metrics. It facilitates threat hunting in massive datasets, enabling security analytics at scale. It minimizes requirements for expertise and training, prioritizes abnormalities, and improves efficiency.

ArcSight Recon Features

- Forensic analysis
- Big Data search optimization
- Customizable reports

Contact us at:
www.microfocus.com

Like what you read? Share it.

Looking for more ArcSight resources addressing the SolarWinds/ SUNBURST attack?

- ArcSight Defends against SolarWinds and FireEye Breaches (Blog)
- ArcSight Response to SolarWinds Supply Chain Attack (video)
- SolarWinds SUNBURST Detection Package
- Implementing Counter Measures in ArcSight for Unauthorized Access of FireEye Red Team Tools
- How To: Using MISP threat intelligence with ArcSight ESM
- ESM Default Content (ArcSight Marketplace)—includes CIRCL MISP threat intelligence, MITRE ATT&CK integrations

Learn more at
www.arcsight.com