Endpoints Are Your Perimeter
How to increase operational visibility with ESM and Sysmon Analytics

In 2017 more than a third of global firms and almost half of U.S. firms surveyed experienced a breach.* If you haven’t already been breached, you eventually will be. Once attackers move past your perimeter defenses, how will you find them if you don’t have visibility at the endpoint layer?

Endpoint detection and response (EDR) solutions are necessary, but they are not enough. Whether it’s from drive-by downloads, phishing, email attachments, social, or other user targeted attacks, your endpoints have become the new perimeter. Once an adversary makes itself at home on one of your endpoints, it works hard to stay undetected collecting credentials, moving laterally across your network for extended lengths of time, and inflicting more and more damage. Unless you have endpoint log collection and SIEM visibility at your endpoints, you’ll be blind to those movements.

Concerns about having enough storage, bandwidth, or computational power in your SIEM to handle endpoint log volumes have become less of an issue with new event collection and cluster technologies. For example, the new Event Broker open message bus in Micro Focus® ArcSight Data Platform (ADP) enables big data scalability with the ability to handle hundreds of megabytes per second of log data. Add to that the distributed correlation in ArcSight Enterprise Security Manager (ESM) 7.0 and you can scale as big as needed by just deploying more nodes, allowing more events than ever before possible to be collected and analyzed.

Track Malicious Endpoint Activity Deeper, Faster, and Easier
In the summer of 2014 Microsoft began including Sysmon (System Monitor) in its Windows Sysinternals Suite of troubleshooting tools. But only recently have security experts have begun to realize how its ability to monitor and record key system activity in Windows event logs can be vital to identifying attackers living on endpoints. Still, effective use of Sysmon data requires help from real-time correlation and analytics tools. That’s why SOC Prime, a MicroFocus Technology Alliance Partner (TAP), has led the way with its development of the Sysmon Framework.

Working with ArcSight ESM, the Sysmon Framework from SOC Prime leverages Sysmon and advanced windows audit logs to heighten your ability to find and track the malicious attack activity living inside your environment. Developed in a security operations center (SOC) lab with SOC-ready content, the Sysmon Framework includes a set of Sigma-based rules that perform a broad set of security checks on endpoint activity and allows you to immediately and easily visualize findings within ESMs dashboards or monitored event channels. Available in the Micro Focus Marketplace, the Sysmon Framework can be deployed on ESM in just a few minutes, allowing new events of interest (EOI) to be immediately directed to SOC triage channels for response and investigation.

The Sysmon Framework from SOC Prime can simplify detection of even well-executed “living off the land” attacks that often allow attackers to hide in plain sight. To increase their stealth and evasiveness, living off the land threats don’t utilize web attack toolkits or known exploits. Instead, to carry out their plans they rely on existing resources on your endpoints, such as executing commands using the PowerShell scripting language that comes with Windows.

Since PowerShell is a native application and its misuse doesn’t require any known malicious tools, its malicious manipulation is extremely

---

* 451 Research, “2018 Thales Data Threat Report”
difficult to detect. But using the Sysmon Framework with ESM makes it easy to spot such activity by identifying PowerShell usage at unusual times by unusual applications or users. For example, if Word or Outlook spawns a PowerShell process, ESM and the framework can alert an analyst to investigate the unusual behavior. In addition to malicious PowerShell usage, the Sysmon Framework can detect a wide variety of other anomalies. It gives you access to 25 other use case monitoring scenarios, such as attacks against KeePass, Mimikatz detection, suspicious driver loads, excessive critical processes running, and more.

Gain Visibility Where Attackers Live
With the SOC Prime Sysmon Framework and ArcSight ESM you have visibility down to where attackers live. You can see how an adversary infiltrated an endpoint and track its movements from one place to another, including lateral movements to other systems. You can spot potentially malicious processes and services. You can uncover the existence of persistence mechanisms and other indicators of compromise. ArcSight ESM and the Sysmon Framework work together to make it easier to find adversaries living on your endpoints, so you can mitigate and remediate faster.

Learn More At
To learn more about how Micro Focus ArcSight ESM and the SOC Prime Sysmon Framework can provide the endpoint threat visibility you need, attend our workshop [insert workshop details] and visit: www.microfocus.com/arcsightactivate or www.microfocus.com/arcsightesm.

Increase endpoint visibility by monitoring Windows Security Logs, PowerShell Logs and Sysmon.