Snare XDR and Sysmon

Whitepaper

Snare XDR and Sysmon

Threat detection software has evolved significantly in recent years. Malware detection and prevention software began incorporating endpoint detection and response (EDR) in a change of tactics in response to more comprehensive, dangerous, and self-masking malware variants. The market has adopted a few different flavours of Detect/Response mechanisms - EDR, Network Detection and Response (NDR), Threat Detection and Response (TDR), and now the industry has settled more on Extended Detection and Response (XDR). The terms have meant different things to different customers and vendors, but the overall goal is to detect and react to threats and unauthorised user activity across networks, servers and endpoints, clouds, and applications. XDR applies analytics and automation to detect, analyse, and hunt for threats in order to remediate or respond to identified threats.

By collecting forensic and log data from a diverse range of system components, correlated data can be scanned to identify patterns across event sources and provide context to a threat or attack chain. Events and activities that would not have been detected or addressed prior to XDR tools and concepts being implemented will be more obvious, allowing security teams to focus on, respond to, and mitigate/eliminate identified threat. This has the benefit of reducing further impact, and dropping the severity, scope, and longevity of the attack.

How Snare helps with XDR

The Snare suite has a comprehensive capability to collect log data from almost any source. Snare agents run on most common platforms such as Windows, Linux variations, MacOS, Solaris, Microsoft SQL Server, and can collect relevant forensic log activity from a wide range of systems and applications. The Snare agents collect and send log data to a Snare Central server and can send or reflect data to a range of other SIEM and analytics tools. The collected logs provide visibility into a range of security-sensitive activities, including:

- Administrative Activity - What actions were undertaken by administrative users? Did they add/remove users, change permissions, change system policies, run privileged commands, etc.?
- Login/Logoff Activity - Who logged on, was it within business hours or out of hours, what systems were impacted? Was it local or remote via a VPN or remote connection to the host? What was the source? Was there lateral user movement between systems? Are users trying to gain privileged access to systems? Are there indications of brute force logins occurring on the network to attempt to guess a password?
- Command Activity - What applications or shell commands were run, were any executed at a higher privilege level? Where were these commands run, on what systems?
- Data Access - What data was accessed, by who? What did they read, change, or delete? Was data copied or exfiltrated to other systems or out over the internet? Was a file or payload or backdoor loaded by malicious actors for later use?

There are various capabilities that help facilitate the analysis of these activities:

- **Collect logs from as many sources as possible –** all servers, desktops, network devices, everything that can send a syslog. All devices should have some form of logging or monitoring in place.
- **Use FIM, FAM, RIM and RAM to track and monitor all key files and system configuration**. Know who and when files were changing and what tools they used.
- **Use Database Activity Monitoring (DAM) to track key activity on SQL databases.** Know if admin accounts are being abused and validate that key data has not been tampered with.
- **Having evidence** to show if the attack vectors came in via email, USB, a web link download, a software update are all important to knowing how they got in.

Another component that facilitates enhanced analysis of activities on Windows systems is the light weight Microsoft "Sysmon" tool. Full details are covered here on the Microsoft site: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

For Windows based platforms, Sysmon provides additional forensic meta data that can enrich the logging and analytics of the Snare Suite. A default install of the Snare Windows agents will collect the Sysmon log data out of the box. As of Snare Central 8.4 we have 26 new report types to cover the events that Sysmon can collect and produce. Customers can also create additional reports for their own use cases, tweaking reports to cope with specific system configurations, or hunt for specific threats.

Some of the additional key functions and attributes that Sysmon enables, include: · Process creation data with full command line for both current and parent processes.

  - Shows the command line switches or parameters that are used, such as passwords or keys used for ransomware to encrypt files or access systems.

- Cryptographic hash of the shell or application binaries executed by users - SHA1 (the default), MD5, SHA256 or IMPHASH.
  - Fingerprinting a file using hashing techniques provides an indication of version history for executed applications.
  - Multiple hashes can be used at the same time.
- Process GUID in process create events o Facilitates correlation of events even when Windows reuses process IDs. o A GUID identifies an object such as a COM interfaces, or a COM class object, or a manager entry-point vector (EPV). o A GUID is a 128-bit value consisting of one group of 8 hexadecimal digits, followed by three groups of 4 hexadecimal digits each, followed by one group of 12 hexadecimal digits.

- Session GUID in each event o Facilitates correlation of events for the same logon session.
- Cryptographic hash of drivers or DLLs that are loaded by the system o Dynamically loading alternative drivers and DLLs can sometimes be used to spoof the normal supported driver/DLL versions.
- Data on raw read access of disks and volumes.
  - Facilitates detection of changes to files and disk volumes

- Network connections, including each connection's source process, IP addresses, port numbers, hostnames and port names.
- Changes in file creation time to understand when a file was really created.
    - Modification of file create timestamps is a technique commonly used by malware to cover its tracks.
- Automatically reload configuration if changed in the registry.
- Rule filtering to include or exclude certain events dynamically.
- Generate events from early in the boot process to capture activity made by even sophisticated kernel-mode malware.
- Provide additional DNS logging to track domain names lookups, and determine what commands and processes are doing these lookups
    - Determine whether it a standard tool, or potentially an undetected malware tool.

Many of the event types provided by Sysmon can overlap with events collected by the traditional Windows audit event log system, providing the ability to correlate and verify actions. Sysmon has capabilities in the areas of administrative activity, logins, process execution, file access and file creation; most of these target areas overlap with the requirements of XDR solutions when tracking and alerting on system and user activity.

There are 27 additional event types Sysmon enables:

1. Process creation
2. A process changes a file creation time
3. Network connection
4. Sysmon service state changed
5. Process Terminated
6. Driver loaded
7. Image loaded
8. Create Remote Thread
9. Raw Access Read
10. Process Access
11. File Create
12. Registry Event (object create and delete)
13. Registry Event (Value Set)

14. Registry Event (Key and Value Rename)
15. File Create Stream Hash
16. Service Configuration Change
17. Pipe Event (Pipe Created)
18. Pipe Event (Pipe Connected)
19. WmiEvent (WmiEventFilter activity detected)
20. WmiEvent (WmiEventConsumer activity detected)
21. WmiEvent (WmieEventConsumerToFilter activity detected)
22. DNSEvent (DNS Query)
23. FileDelete (File Delete Archived)
24. ClipboardChange (New content in the clipboard)
25. Process Tampering (process image change)
26. FIleDeleteDetected (File Delete logged)
27. 255 Errors from Sysmon

For the full details on each, refer to the Microsoft link above.

These additional tracking and forensic log details enable, extend, and enrich Snare log data. The extra content facilitates additional reporting and threat detection and hunting capabilities within Snare Central to support:

- The detection of malicious activity on the network
- Meeting the requirements of frameworks such as "MITRE ATT&CK" o https://www.snaresolutions.com/portfolio-item/mitre-attack/
- The enhancement of DNS log data o https://prophecyinternational.atlassian.net/wiki/spaces/Snare/pages/897417517/H ow+to+Collect+DNS+Logs