Chapter 6 - Security Event Generation And Collection

A small blind spot could be a doorway to a future attack. Therefore best practices are to layer security monitoring points across the network and monitor all events from a centralized data-collection solution.

Data Collection

It is important to properly size your data-collection solution for the number of expected data-generating products on your network.

To properly size the solution:

- How many devices are sending Data
- How many events per second
- What are the Data-retention requirements for captured data

Calculating EPS

The most accurate way to determine EPS is to place a syslog server on the network and measure for a specific time.

The Kiwi syslog server is a good option, but requires a license. The Ubuntu SysLog Server is a free alternative.

Ubuntu Syslog Server

- Download and install the `syslog-ng` server
- Configure the server to receive messages from data-generating devices
  - `syslog-ng` configuration file: `/etc/syslog-ng/syslog-ng.conf`
- Specify a folder to capture logs: `/var/log/eventdata.log`
- Restart the server: `sudo /etc/init.d/syslog-ng restart`

You can also log specific devices, such as firewalls or routers. Setting the logging level will enable more or less logs to be sent to the log file. A log level of 7 will send debugging information. A log level of 1 will send only Emergencies (Unusable system)

If you are preparing for a new network, decide what level you are going to use, but realize you are probably guessing.

Once we know the level of event we want to log, we can use EPS formulas.

- `EPS = Number of System Events / Time Period in Seconds`

Peak EPS is necessary to identify when a incident is taking place.

Important factors:

- *Expected Number of Peaks:* Number of Peaks experienced by the network (Normally, 3. Morning logins, Lunchtime brakes, end-of-business wrap-up)
- *Duration of a peak:* Duration of the Peak
- *Deviation Factor:* Average deviation between normal EPS.

$$TotalPeakEPSperDay = \frac{NormalEPS * ExpectedNumberofPeaks * DurationofaPeak(Seconds) * Deviationfactor}{86{,}400(Secondsinaday)}$$

Given the amount of guesswork, build in at least 20% margin to ensure you have enough space and process power on your data collection solution.

Also, make sure to correctly configure accurate time synchronization between products.

Network Time Protocol

There must be order to how data is categorized. To use proper time synchronization, use a NTP server.

NTP reads the time from the authoritative resource and distributes it across the network so that all devices are in proper synchronization for time.

The recommended number of NTP servers to synchronize is 3, to be able to apply an agreement algorithm.

NTP includes checks to validate a system before syncing.

Deploying NTP

There are three ways in which you can deploy NTP:

- *Client/Server:* Client dependent on the server, which is synchronized to a group member.
- *Symmetric active/passive:* Group of low stratum peers acting as a backup for each other.
- *Broadcast:* Broadcast server to broadcast time over a local subnet address.

Data-Collection Tools

User Interface Experience

Remember, when installing a SIEM, it's your network, so it is important that you know how to operate it.

Firewalls

As the technology has evolved, new types of firewalls have appeared.

Stateless/Stateful Firewalls The first firewalls performed static packet filtering. This made these firewalls vulnerable to IP spoofing.

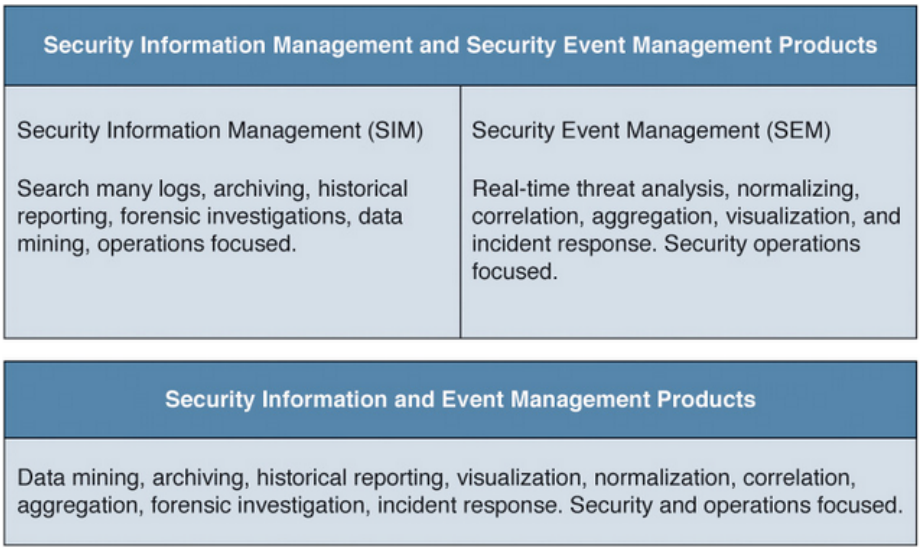

Figure 1: SIEM, SIM, SIM

Stateful packet inspection was later added to examine the packets rather than only applying filtering.

Logging options:

- Permitted connections by the Firewall
- Denied connections
- Denied rule rates
- User authentication and command usage
- Cut-through-proxy activity
- Bandwidth usage broken down by connection
- Protocol and port numbers
- Network Address Translation (NAT) or Port Address Translation (PAT) auditing

A popular stateful firewall: Cisco Adaptive Security Appliance ASA

Application Firewalls Inspect traffic at the application layer of the OSI model. The value is that it can capture more details about the traffic, such as: User X is on the internal network on a Windows XP trying to access FarmVille using a Firefox browser. This provides a lot more information.

The **Challenges** are that the deeper the inspection (Like SSL decryption) the more resource-intensive the process is, and the bigger the lag.

Cloud Security

As technology becomes Internet-capable, CISCO has provided SaaS Firewalls, where all traffic is routed through their firewall. (Cisco Meraki)

Virtual Firewalls

> A virtual firewall (VF) is a network firewall service or appliance that operates within a virtualized environment and provides similar security features of a physical firewall.

Common mistakes in data center security strategies are not considering security solutions for internal compute (that is, just focusing on what enters and leaves the data center) and assuming any vendor firewall can function properly for a data center environment.

Host Firewalls

Most modern OS have virtual firewalls configured with default parameters. It is rare for a SOC to collect host system firewall logs unless the admin is troubleshooting this particular system.

Intrusion Detection and Prevention Systems

> An intrusion detection system (IDS) is used to monitor a network or system activities for indications of malicious behavior or policy violations

Network IPS solutions are always deployed inline with the traffic of interest. Network IDS systems are most commonly placed off a tap or SPAN port that views a copy of the traffic of interest. It is common for administrators to not take into consideration Network Address Translation (NAT)

IPS and IDS systems use the following methods to detect threats:

- *Signature-based detection:* Compares traffic, files, or behavior against a known list of attack signatures.
- *Statistical anomaly-based detection:* Also behavior-based detection looks for abnormal behavior from network trends.

By combining both types of detection, IPS/IDS technology can be very effective at catching known and unknown threats.

IPS/IDS systems:

- Cisco FirePOWER IPS
- Cisco Meraki IPS
- Snort

Host-Based Intrusion Prevention

Normally come bundled in an Anti virus solution, alongside with anti virus, Firewall, IPS.

Routers and Switches

A switch forwards data looking at a physical device address.

A router forwards packets by locating a next hop address.

Router and switch logs are very important, and commonly overlooked.

Host Systems

Typically Host Systems are end-user laptops or mobile devices. Securing Host Systems typically means installing security applications. You can use open source applications, such as IPTables as a host-based firewall.

Most security vendors provide applications for Windows, Mac, and Android, but not for Linux.

Host security products offer:

- Firewall
- Intrusion detection/prevention
- Antivirus
- Web security

Use a centralized system to collect logs (SNMP, syslog), rather than pulling from individual devices.

Mobile Devices

The most common security platforms used for managing polices on mobile devices are Mobile Devices Management MDM platforms. They tend to take two different approaches:

- *Sandbox approach:* Creates a isolated environment that limits what applications can be accessed and controls how systems gain access to the environment.
- *Endpoint management:* This strategy requires an agent to be installed on the mobile device to control applications and to issue commands such as remotely wiping sensitive data.

Breach Detection

Focus on identifying activity of malware inside a network after a breach has occurred

Vendors with breach-detection offerings include Bit9, FireEye, and Mandiant.

Web Proxies

> Web proxies act as an intermediary between a host systems and the Internet. Web proxies work by intercepting traffic between two sources such as the inside network and the Internet. It is critical that the web proxy solution be configured properly before pushing traffic to it to avoid end-user interruption of services. This includes identifying all ports and protocols that will be associated with the web proxy.

Types of proxies:

- CISCO Web Security Appliance (Physical proxy)
- CISCO Cloud Web Security (Cloud Proxy)

Cloud Proxies

Adds web security using a SaaS to enforce a security policy. This is accomplished by routing traffic through the cloud security solution.

DNS Servers

> A Domain Name System (DNS) server is a database that provides mapping between hostnames, IP addresses (both IPv4 and IPv6), text records, mail exchange, name servers, and security key information defined in resource records.

Each query to the server contains 3 pieces of information:

- Fully Qualified Domain Name (FQDN)
- A query type that can be a specific resource record by type or specialized type of query operation
- A class for the DNS name

Exporting DNS

Can be valuable to the SOC, as it can accurately view all Internet traffic activity from users and devices. From this data, you can analyze anomalies, such as a system, communicating to both internal, and external devices. As this traffic is distributed, and you don't control the ISPs it is going to be complicated to obtain all DNS traffic.

Network Telemetry with Network Flow Monitoring

Network flow monitoring, commonly called NetFlow, can be enabled on standard network and security products, essentially turning your network into a giant sensor.

NetFlow Tools

NetFlow security tools rely on trends found from monitoring network behavior. For this reason, most NetFlow tools require at least a week's worth of data before they can distinguish what is considered normal and unusual behavior.

NetFlow tools can see data from many sources and need to be tuned to understand the environment being monitored.

StealthWatch

StealthWatch is a NetFlow analyzer. It provides the users with information and deep inspection based on network flows. If paired with the CISCO ecosystem, it can even monitor known C&C servers to see if a machine from your network has connected to it.

NetFlow From Routers and Switches

NetFlow from Security Products

Many security products such as firewalls and intrusion prevention solutions produce NetFlow. It can be valuable to leverage NetFlow as a method to expand the solution's detection capabilities and fill in the gaps between network segments. For example, a security solution may be able to detect various forms of attack, yet not recognize a possible unauthorized data breach based on data leaving a critical system for the first time to an unusual system.

NetFlow in Data Centers