Sizin İçin NEFER SAVUNMA A.Ş.

nefersavunma.com.tr

Detecting attacks with

SureLog

Twelve Real World Use Cases for SIEM

Twelve powerful SIEM use cases to kick-start your security program

The rising trend in the number and types of attacks has driven enterprises to adopt SIEM as a proactive measure for threat management. This eBook talks about the use cases that every enterprise should practice at the minimum to reap the true benefits of a SIEM solution.

Through the combination of scenario- and profiler-based analytics, use SureLog to effectively deliver full-spectrum analytics and enable comprehensive monitoring for threats known and unknown.

Detecting anomalous user account creation

Attackers often operate by first gaining access to a privileged user account, creating a temporary backdoor account for themselves, using that account to secretly access some critical resource on your network, and finally they delete this account and leave without a trace. Backdoor accounts are serious threats as they might be used for anything from data theft to privilege abuse.

While the ways hackers gain initial entry to your network and the types of malicious activity they can perform vary, you can check for backdoor accounts by looking for anomalous user account creation.

How SureLog detects backdoor accounts:

SureLog monitors privileged user activity throughout devices on your network. Its correlation engine discovers anomalies in privileged user activity by identifying any user accounts that were both created and deleted within **24 hours**.

Legitimate accounts are created or deleted in a planned manner, so a random account being created and deleted in a short time frame is definitely suspicious.

SureLog raises an alert in real time once it detects an anomalous user account, generating an incident report that includes details about the anomalous account and the privileged account used to create it.

Detecting malware infections

The threat landscape is constantly changing. Threats come from internal as well as external sources and organizations are under tremendous pressure to manage these threats. Attackers rely on malware when trying to establish an initial foothold. Threat intelligence is knowledge that helps you identify security threats and malwares.

How SureLog detects malwares with Threat Intelligence

Here at SureLog, The resultant data that you obtain after enriching the events with threat intel is further validated by running a lookup against it. Thus it can be said that lookup gives additional details about something that has been deemed malicious by the integrated intel plugins.

Detecting brute force attacks

Brute force attacks are one of the most basic but effective methods used to hack accounts on a network. In a typical brute force attack, an intruder tries to gain access to a device in your network by entering various logon credentials until one succeeds. Sophisticated brute force attacks implement automated techniques to try out different password combinations in quick succession. This trial-and-error method can prove deadly if unchecked.

How SureLog detects brute force attacks:

SureLog scans logon events of critical servers and workstations with high priority. By default, the solution's correlation engine identifies when a single device experiences twelve failed logons within twelve minutes, followed by a successful logon within the next minute. If it detects such an attack, it raises an alert and creates an incident report with details about the breached device and logon events.

Domain Generation Algorithm detection

Malware that rely on a fixed domain or IP address can be detected quickly and blocked immediately. This poses as a big hurdle to the attacker's operations. In such scenarios, Domain Generation Algorithms (DGAs) are used to generate and register many different domains for their Command-and-Control (C&C) server. So most modern botnets would rather switch to a new domain at regular intervals to protect their domain from black-listing attempts, instead of bringing out a new version of the malware or setting everything up again at a new server.

How does DGA work?

A DGA periodically generates a large number of random domains that resolve to the C&C server of a botnet. Ordinarily, with a botnet using a static domain for its C&C server, you could easily takeover the botnet and blacklist its domain. With the help of a DGA that periodically generates a new domain for the bot's C&C server, it wouldn't make sense to takeover a domain that isn't being used by the bots to build a connection.

How SureLog detects DGA:

The nature of the DGA makes it difficult to detect with signature or reputation based detection and prevention systems. An intelligent system is required to detect a DGA. At DNIF, we extract domain name, perform thorough analytics to detect DGA status, check registration status and the domain reputation of the suspected domains.

UEBA Profiler at SureLog

Abnormal user behavior - Unusual login attempts

Take for instance a user X logs on to his system 10 times a day. Now if user X logs in approximately 30% (can be varied as per requirement) more times than usual then we might say this is an unusual activity for the user and raise an alert for it.

Abnormal user behavior – Anomaly on authentication behavior

If any user's daily successful login to failed login ratios deviates from regular days, it will be considered suspicious.

Suspicious movement - Dormant user access

Dormant and inactive accounts are often an easy target for attackers because there is little visibility on these accounts.If any user activity is observed after suppose 60 Days of the user being dormant, it will be considered suspicious.

First time activity - New device detected

SureLog monitors all the devices for the first 14 days and if there is a new device in the network, raise alert for it.

First time activity – New VPN location

If a VPN activity from a location for the first time detected, raise alert for it.

Suspicious traffic – Unusual HTTP protocol usage

If any user activity is observed whose HTTP to DNS protocol ratio is %300 more than %95 of the other users for the last four-week ratio, raise alert for it.

Suspicious firewall traffic – Unusual internet activity

If the same user blocked by the firewall 30 times within **30 days**, raise alert for it.

Intelligent brute – force attacks – Unusual user behavior

A user wants to eliminate classic SIEM rules, such as detect if there are 3 failed logins in 5 minutes or 20 minutes. if a user tries to log in to the same machine for at least three, four days without any successful login, at least four-five hours intervals (not to be detected by well-known and legacy SIEM rules like if there is three authentication failure within thirty minutes from the same user to the same machine), raise alert for it.