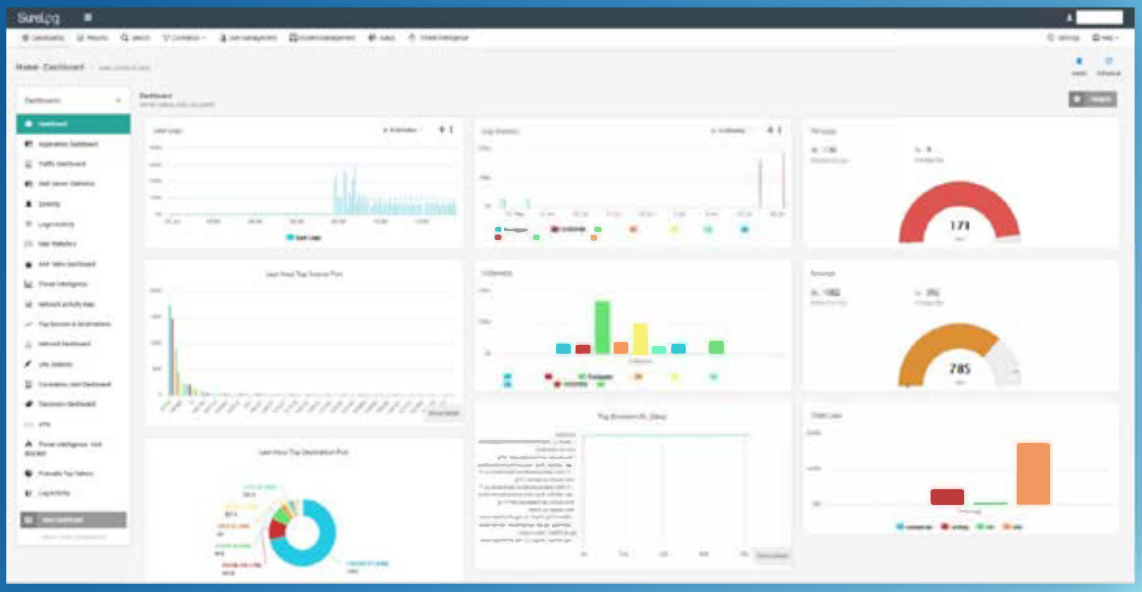
Sizin İçin NEFER SAVUNMA A.Ş.

nefersavunma.com.tr

SureLog SIEM
Intelligent Response Feature

SureLog

SIEM solutions are responsible for the automated analysis of events, which sends alerts to the concerned security team for notifying them about the immediate issues and taking automated actions in parallel.



SureLog Dashboard

The correlation systems consist of **two parts.**

1. Detection **2. Response**

The response part is divided in two sub-parts as alarm and taking action.

SureLog Intelligent Response provides built-in incident response with configurable automated actions. SureLog detects malicious IPs, users, machines, processes and performs incident response in a timely and effectively manner.

SureLog can do much more than trigger email alerts or sending SMS alerts.

SureLog is designed to immediately respond to security, operational, and policy-driven events using predefined responses, such as quarantining infected machines, blocking IP addresses, killing processes, and adjusting Active Directory settings.

The response module automated actions are:

- Send email
- Send SMS
- Block IP

- Disable user
- Shutdown machine
- Kill process
- Adjust Active Directory settings
- Execute a script

    - ☛ Visual basic script
    - ☛ Batch file
    - ☛ Perl script
    - ☛ Python script
    - ☛ Any executable

        - ✓ Executing java code
        - ✓ Running application
        - ✓ Etc.

- Send SNMP Trap
- Open ticket
- Update dynamic lists. For example, adding or removing IP address in forbidden IP address list. Dynamically updating this list for those who try more than 3 failed logon accesses in last week, or adding a benign IP or URL that triggered an alarm to a Whitelist so that false positives aren't generated in the future.

SureLog Intelligent response actions can use any parameter that is available on SureLog schema. For example:

- Event source IP
- Event destination IP
- Username
- ComputerName
- ProcessName
- DomainName
- SourcePort
- DestinationPort
- Etc.

One or more parameters and any combination of the SureLog schema can be used (Source IP, Username, etc.) to give an intelligent response.

The machine attacked can be shutdown by using the necessary scripts or the list defined before can be updated or a new list can be defined and these lists are used automatically by the other rules or the rules added newly or get done another process requested.

Dynamic list updating and defining is a feature of SureLog which are not provided by any other product in the world. This feature allows incredible flexibility and wide range of uses for the Detection module. For example, Warn if a user in Administrator group tries failed logon attempt. Here, Administrator group is kept up to date dynamically with the other rules. For example, if a user is added in Admin group, update Administrator user list.

Tracing a correlation result saves time from hours to days. For example, you have a use case like if a user created and the same user has failed authentication many times and then authenticate successfully. If your SIEM solution does not give the details of user creation event like who is the creator or does not give the details of authentication failures and gives details of just success authentications, then you have to search your logs to find user creation details, authentication failure details and waste time.

failures and gives details of just success authentications, then you have to search your logs to find user creation details, authentication failure details and waste time.

Many SIEM solutions just give the latest part of the correlation rules. With SureLog's advanced correlation tracing feature- Which is the part of Intelligent Response-, it is so easy to trace the detection logic from start to end.