encode
cyber threat management

Datasheet

Enorasys SOCStreams

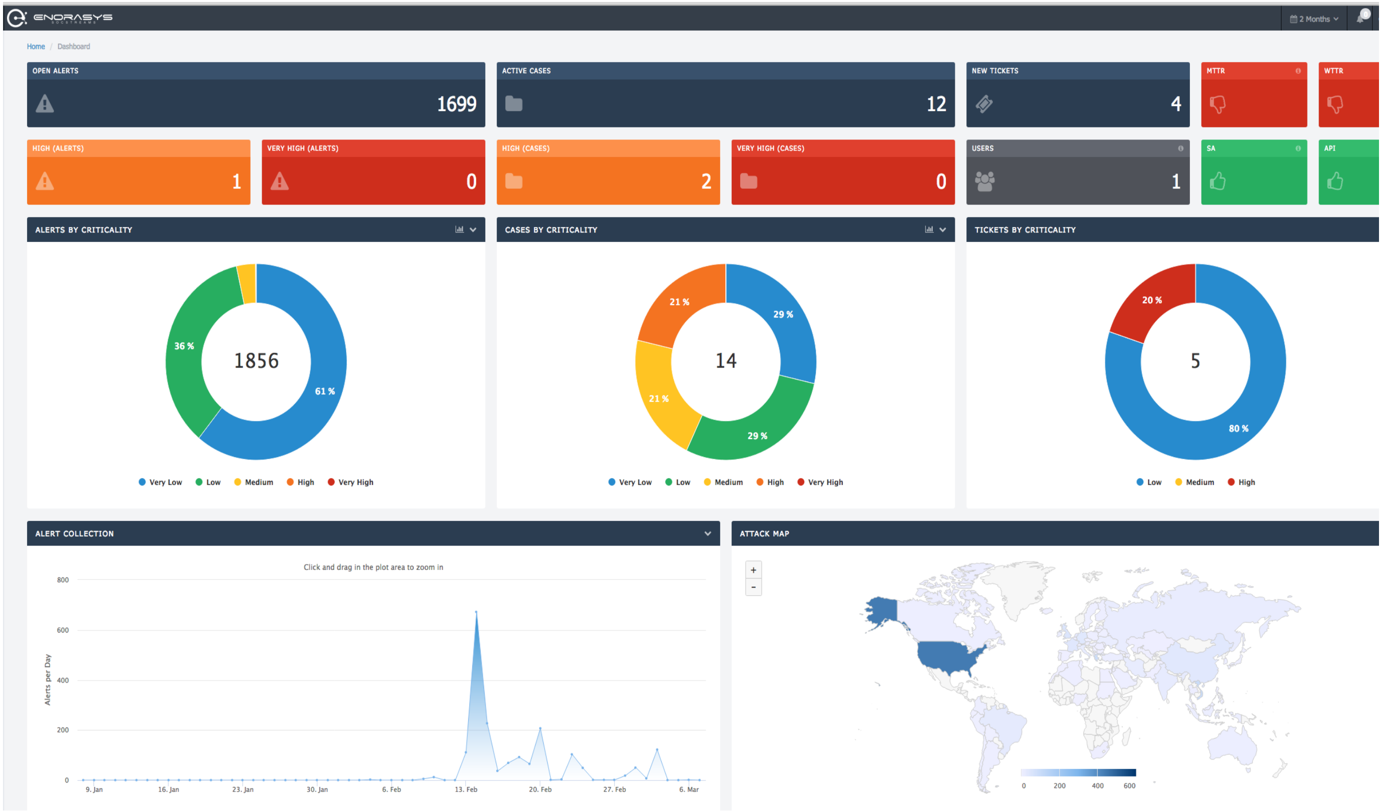
Security Incident handling and orchestration

Key Benefits

Enorasys SOCStreams Response Orchestration system provides advanced Incident Lifecycle Management. It achieves this by encapsulating and streamlining all core Security Operations Center (SOC) and Cyber Incident Response Center (CIRT) processes.

SOCStreams in combination with its Adaptive Threat Response (ATR) engine takes Incident Response a step further by providing SOC/CIRT analysts with a centralized focal point for process integration and the tools required to orchestrate responses. This ranges from security alert handling to targeted investigation and response.

SOCStreams can constitute the main interface for both SOC service users and SOC personnel alike. Service users are provided with instantaneous views of the security events raised for their environment, actions taken to manage them and corresponding status, along with response guidelines and relevant KPIs.



Transforms your SIEM deployment to a full SOC

SOCStreams helps transform your SIEM deployment to a full SOC through embedded processes, intuitive workflows and knowledge based articles for security event handling, investigation and response.

Key Benefits

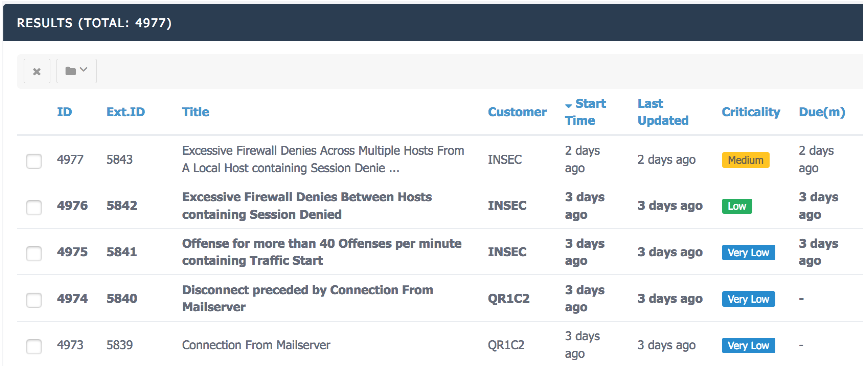
SOCStreams provides step-by-step SOC operations playbooks and use case management. When combined with extensive integration capabilities, SOCStreams ensures minimum time to value and maximum return on investment (ROI).

Ensures SOC effectiveness

Consistent efficiency and effectiveness are the key objective of a SOC. SOCStreams provides just that, by automating and streamlining SOC processes for effective management of the complete lifecycle of security alerts and verified incidents.

Automates targeted investigation and response

Upon threat detection, SOCStreams' ATR engine enables the SOC/CIRT team to perform targeted remote alert investigation and incident response. SOCStreams thus minimizes the response to a potential compromise through its ATR engine and third party systems integration.



RESULTS (TOTAL: 4977)

	ID	Ext.ID	Title	Customer	Start Time	Last Updated	Criticality	Due(m)
□	4977	5843	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Session Denie ...	INSEC	2 days ago	2 days ago	Medium	2 days ago
□	4976	5842	Excessive Firewall Denies Between Hosts containing Session Denied	INSEC	3 days ago	3 days ago	Low	3 days ago
□	4975	5841	Offense for more than 40 Offenses per minute containing Traffic Start	INSEC	3 days ago	3 days ago	Very Low	3 days ago
□	4974	5840	Disconnect preceded by Connection From Mailserver	QR1C2	3 days ago	3 days ago	Very Low	-
□	4973	5839	Connection From Mailserver	QR1C2	3 days ago	3 days ago	Very Low	-

A tool in the hands of the SOC Analyst

The everyday tasks of a SOC analyst are handled in a single place thus increasing effectiveness and streamlining security event monitoring, handling and incident management processes.

SOCStreams provides the analyst with a clear and dynamic view of the current security event status against multiple monitored environments. Analysts can easily action an event, delegate it to one of their peers, escalate to second level SOC Analysts and notify the appropriate points of contact for the monitored environment. This is all done through a single application view- increasing the efficiency of the analyst while reducing the time to respond at the same time.

Multitenant and multiplatform integration

SOCStreams provides full multitenant views and dashboards along with role based access control and user provisioning and management for simultaneous support of multiple monitored environments. In addition, the software supports integration with multiple SIEM systems and third-party service desk applications through an extensive bidirectional API and out-of-the-box connectors for major vendors. SOCStreams also supports MS Active Directory LDAP integration for authentication and authorization.

Key Benefits

Automates and streamlines SOC processes

From security event assignment to SOC/shift-handover and SLA/OLA management, SOCStreams makes certain correct processes will be followed.

This is achieved through use of embedded workflows and knowledge base articles for security event handling and incident response. This includes step-by-step playbooks for SOC operations and Use Case management, embedded processes for SOC/shift-handover and SLA/OLA measurement and reporting.

> SOCStreams' Adaptive Threat Response (ATR) engine provides an integration layer with endpoint visibility and control sensors and third-party network security gateways.

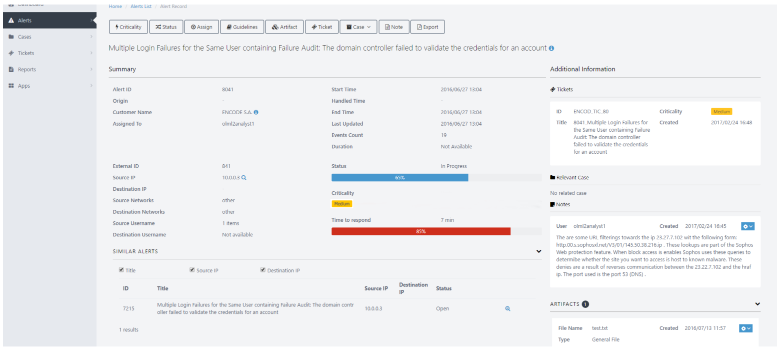
Adaptive Threat Response

SOCStreams' Adaptive Threat Response (ATR) engine provides an integration layer with endpoint visibility and control sensors and third-party network security gateways.

Combined with Adaptive Threat Response (ATR) engine, SOCStreams provides SOC analysts and Incident Response teams with the means to further investigate suspicious activity and respond early to security incidents. The ATR engine can be invoked directly by security analytics/monitoring systems or manually by SOC analysts to provide additional on-demand context. This provides the situational awareness required by analysts for verifying security events and taking follow-on actions, ranging from ongoing monitoring to containment.

Users focal point

SOCStreams provides SOC customers and Service Users with a focal point where all service related communications and service management activities are performed and/or tracked. Security Event and Incident notification, reports management, service requests, SLA/OLA reporting can all be accessed or performed through a single interface with clear and dynamic dashboards and searchable views. Service users can have immediate view of security events raised for their environment, actions taken to manage them and corresponding status along with other service-related information and key performance indicators (KPIs).



Multiple Login Failures for the Same User containing Failure Audit: The domain controller failed to validate the credentials for an account

Summary

Alert ID 8041
Origin -
Customer Name ENCODE S.A.
Assigned To olml2analyst1
Start Time 2016/06/27 13:04
Handled Time -
End Time 2016/06/27 13:04
Last Updated 2016/06/27 13:04
Events Count 19
Duration Not Available

External ID 841
Source IP 10.0.0.3
Destination IP -
Source Networks other
Destination Networks other
Source Username 1 items
Destination Username Not available
Status In Progress 65%
Criticality Medium
Time to respond 7 min 85%

SIMILAR ALERTS

☑ Title ☑ Source IP ☑ Destination IP

ID	Title	Source IP	Destination IP	Status
7215	Multiple Login Failures for the Same User containing Failure Audit: The domain contr oller failed to validate the credentials for an account	10.0.0.3		Open

1 results

Additional Information

Tickets

ID ENCOD_TIC_80
Title 8041_Multiple Login Failures for the Same User containing Failure Audit: The domain controller failed to validate the credentials for an account
Criticality Medium
Created 2017/02/24 16:48

Relevant Case

No related case

Notes

User olml2analyst1 Created 2017/02/24 16:45

The are some URL filterings towards the ip 23.27.7.102 wit the following form: http.00.s.sophosxl.net/V3/01/145.50.38.216.ip . These lookups are part of the Sophos Web protection feature. When block access is enables Sophos uses these queries to determibe whether the site you want to access is host to known malware. These denies are a result of reverses communication between the 23.22.7.102 and the hraf ip. The port used is the port 53 (DNS) .

ARTIFACTS 1

File Name test.txt Created 2016/07/13 11:57
Type General File