SECURITY INFORMATION & EVENTS MANAGEMENT (SIEM)

COMPREHENSIVE SIEM SOLUTION

AEGIS SIEM platform collects, analyzes and correlates data with the ability to deliver threat detection, compliance management, incident response, threat intelligence, and SOAR capabilities, complete with messaging and ticketing system for a unified security platform

ENDPOINT DETECTION & RESPONSE

Focused on providing the right visibility with the insight to help SOC Team discover, investigate and respond to threats and attack scenarios across multiple endpoints.

DEVICE INTEGRATIONS

Integrates with different infrastructure, security devices and operating systems. Enables users to bring other service logs into their platform allowing for quick tirage and visuals amongst various log sources.

SECURITY DASHBOARDS

Quickly drilldown into individual host's processes or view activity on all of your endpoints with our detailed customizable security dashboards.

CUSTOM RULES & DECODERS

SIEM rules are highly customizable, to detect events type and trigger a response using the MITRE ATT&CK framework. Aggregating security data is complex, and without the right decoder, logs will not be recognized. Customizing decoders normally cost high, but our services include customizing decoders at no cost.

FILE INTEGRITY MONITORING

A critical layer of file, data, and application security that detects and generate alert for file and directory integrity monitoring. It provides data security and integrity to critical and sensitive business information.

DFIR-IRIS TICKETING SYSTEM

Digital Forensic and Incident Response ticketing system is a collaborative platform for Incident Responders that provides ability to collect, splice, and analyze evidence for centralized investigation results. It comes free with the SIEM solution for the SOC to manage and maintain investigation ticket information in a single location

SOAR - SECURITY ORCHESTRATION, AUTOMATION & RESPONSE

Automate complex tasks, search and process high volumes of data quickly, and consistently alerts you of high impact incidents. Reduces response time, and provides consistent efficient automated reports

THREAT INTEL

AEGIS SIEM analyzes all relevant metadata in security events, extracts observables and executes threat intel to pinpoint indicators of compromise in real time. Domains, file hashes, IPs, etc. are cross referenced to our open-source and free threat intelligence platform

INCIDENT REPONSE PLAYBOOKS

Minimize negative impacts and restore data, systems, and operations back online with the collection of incident response playbooks that the SOC can use. Highly detailed, pre-planned procedures to be followed when cyber security incidents occur.

AEGIS
SIEM & SOAR

SIEM FEATURES

SPEED OF IMPLEMENTATION

Seamlessly integrates with your network be up running within days, not months. Deliver instant results through visibility of events and threats

COMPREHENSIVE VISIBILITY

See everything happening in your environment and normalize it efficiently. Obtain, and maintain all-inclusive visibility of your infrastructure and user activity.

RAPID IDENTIFICATION

Quick identification and resolution of risks, a unified security information and incident management platform

REDUCED OPERATIONAL RISK

Process automation delivers live compliance dashboards, reporting and security workflow to streamline analyst activities

EDR & XDR FEATURES

EDR (Endpoint Detection and Response) and XDR (Extended Detection & Response) platforms provide centralized alert system that can group related log alerts from multiple systems into a single interface, which also include machine learning functionalities that help defensive capabilities adapt to any given technology threat.

ACTIVE RESPONSE

Investigate threats and deploy various countermeasures to neutralize persistent threats. Active response capability is to mitigate threats or gather any additional data to aid later diagnostic processes immediately after an alert is raised.

INTEGRATED THREAT INTELLIGENCE

Helps you to understand what to look for and what others have discovered through community shared threat intelligence

RAPID RESPONSE & SOLUTIONS

Advanced real-time collection, analysis and threat detection with live dashboard and automated alerting. collects and automatically correlates data across multiple security layers

DEEP FORENSIC INVESTIGATION

Logged data represent the digital fingerprints of all activity that occurs across IT infrastructure, it can be mined to detect security breach, covert characteristic of attack tools, techniques and procedures (TTPs).

UNLIMITED STORAGE

No cost for any storage increases, no storage limits, the organization can define storage limits based on their requirements.

NO VENDOR LOCK-IN

No business or operations disruption, when you want to change service and maintenance provider. No license management, software are free and support is abundant.