encode
cyber threat management

Datasheet

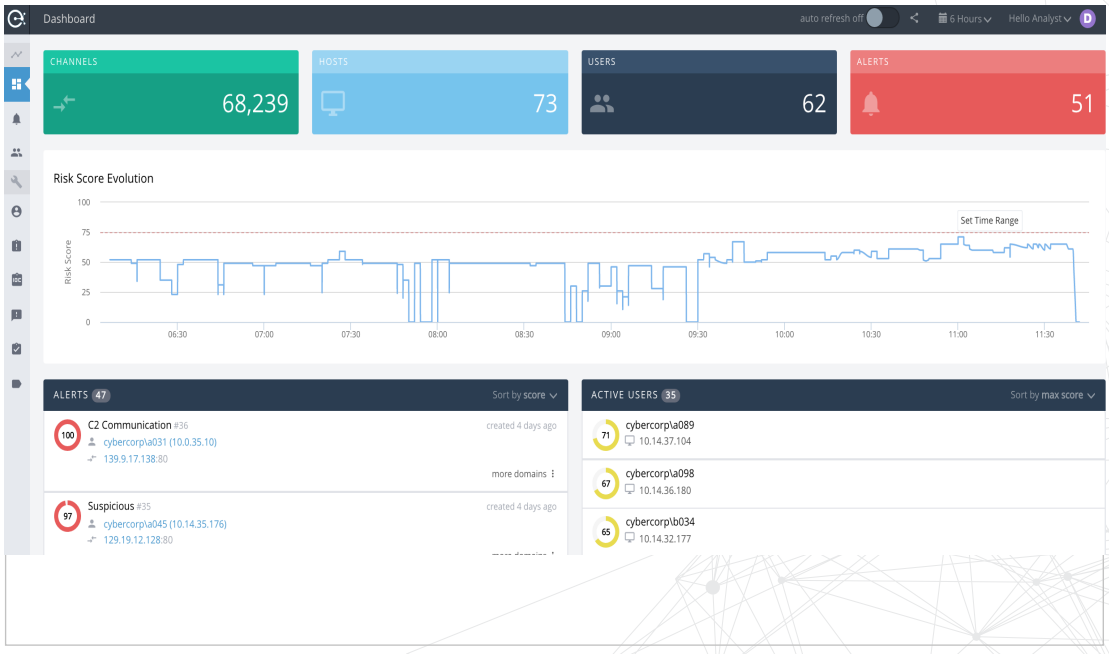
Enorasys Security Analytics

Finding the needle in the needle-stack

Enorasys Security Analytics is a leading predictive security analytics solution designed from the ground up to deliver early compromise detection by understanding the "attack logic" and exploitation path of an advanced and determined adversary. This is realized through "focused" Big Data Security Analytics harnessing powerful machine-learning techniques and encapsulated offensive and defensive expertise.

Enorasys Security Analytics is continuously analyzing and modelling relevant activity. Through a unique analytics approach that combines pattern detection with activity profiling and external/ environment-specific context, Enorasys Security Analytics assigns risk scores to users, network nodes and corresponding activity attributes.

The system goes one step further by correlating such risk scores to effectively connect the dots to attack paths. This allows for both backtracking an attack to its origin and the continuous monitoring of its evolution and extent over time- until it is properly contained or eradicated.



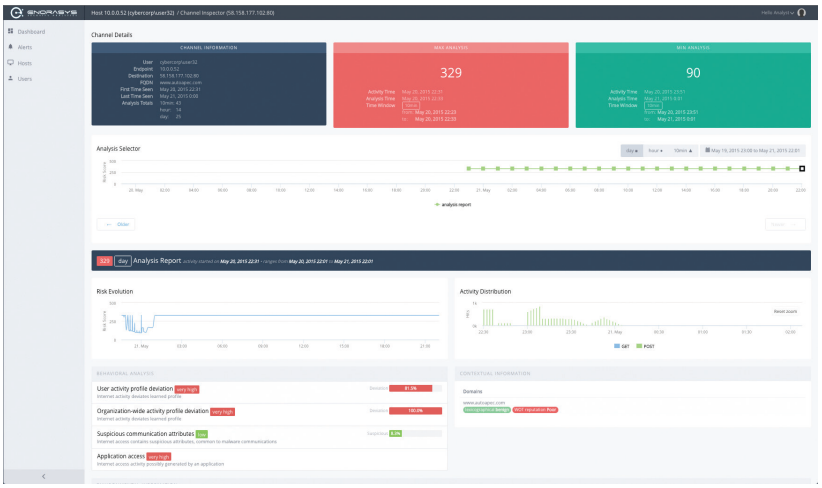
Key Benefits

Security Intelligence...that matters

Augments your early warning capabilities with unprecedented insight into activities happening in your network thus providing security intelligence that matters…the one that relates to your unique environment.

Automates the "proactive threat hunting" process

Built by experts in data analytics, cyber offensive techniques and cyber security operations, Enorasys Security Analytics effectively automates the "proactive threat hunting" process. This provides Security Operations Center (SOC) teams with the means to hunt and track down hard-to-spot malicious activity as never before.



A Security Analytics platform – not a point solution

Runs on top of and leverages big data analytics platforms and comes with a set of canned security analytics modules. Each module provides continuous risk scoring of user and network node activities relating to different phases of the attack kill chain. Analytics modules encapsulate our extensive offensive and defensive expertise, and are constantly updated and extended for additional use case coverage.

Powerful Analytics & Risk Scoring Process

Employs a unique combination of pattern recognition with user and network node activity profiling correlated with external/ environment-specific context data. This ensures our canned analytics modules are able to use the right tool for the right job for each use case and corresponding monitored activity.

Self-Learning

Automatically builds adaptive profiles of "learned normal behavior" and detects deviations and complex attack patterns against large sets of data over time. Moreover, the risk-scoring process is self-optimized for each monitored environment through security analysts' feedback on detected suspicious activity.

Embedded Offensive & Defensive Expertise

Encapsulates Encode's unmatched insight into targeted cyber-attacks gained through hundreds of APT simulation and red teaming exercises delivered over the last decade. Analytics modules and more specifically, pattern detection algorithms leverage our extensive knowhow on attack

Tactics, Techniques & Procedures (TTPs), along with the ongoing research by our Threats Labs into new evasion and attack techniques.

Threat Hunting & Visualization

Designed by security analysts for security analysts. Enorasys Security Analytics provides advanced visualization of risk scores and threat activity along with a complete toolbox for fast and intuitive investigation of suspicious activity. The system can feed existing Security Information & Event Management (SIEM) systems with alerts for high-risk activity. Further investigation can be done through the analyst interface invoked through the SIEM console.

Footprint and time to value

Security Analytics is an agentless solution - it consumes existing logs and can also leverage data from third party security sensors. This means a minimal footprint inside the network. Due to out-of-the-box integration with Splunk Enterprise, the solution can also immediately leverage any existing investment in Splunk deployments.

Flexibility

Provided as a managed service through our 24x7 Cyber Operations & Intelligence services, It can also be deployed as a Cloud/SaaS or on-premises solution for organizations that want to enhance their current SOC with unprecedented security insight through advanced security analytics.

Scalability

Vertical and horizontal scaling allowing analytics to cope with tens of thousands of users, network nodes and vast amounts of data.

Enorasys Security Analytics comes with a set of pre-packaged security analytics modules. Each one provides continuous risk scoring of specific user and network node activities that have been designed and built with a focus on providing true early warning against targeted, evasive cyber-attacks, commonly known as “Advanced Persistent Threats” (APTs).

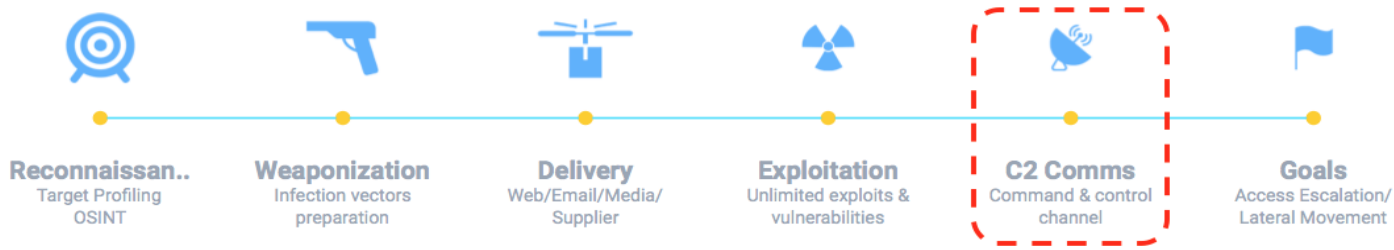
Use Cases & Analytics Modules

C2 communication detection

The iAccess security analytics module analyses Internet access activity to provide early detection of Command & Control (C2) communications by Malware and Remote Access Tools (RATs) on user endpoints and servers regardless of infection or exploitation vector used.

The module processes logs generated by proxies, secure web gateways and egress firewalls. It then combines pattern detection, user profiling and external context data for calculating risk scores of each and every Internet access and corresponding user and network node.

Since foothold establishment is corner stone of any targeted cyber-attack in the early phase of the Cyber attack process, iAccess analytics essentially provides the earliest warning possible for such a successful attack.



Architecture

The solution follows a distributed architecture:

Collection Layer: The collection layer comes in the form of a virtual appliance that collects relevant data (e.g. logs), either directly from the systems that generate the data or through an existing repository (e.g. SIEM system) that forwards data to the event processor/Big Data analytics engine.

Event Processor: Enorasys Security Analytics runs on top of and leverages big data analytics platforms. Currently we support Splunk Enterprise as the event processor/Big Data analytics engine, but the system's abstract log query layer can support a variety of engines (e.g. Elastic Search, Hadoop etc.).

Security Analytics Engine: The Security Analytics engine has three major components, namely Risk Engine, Database and Management console. They can operate in all-in-one mode (1 server with all components) or in a distributed architecture with multiple Risk Engines (or instances) and with one central Management Console and Database. When the solution is provided as a managed service, through our 24x7 Cyber Operations & Intelligence services or as a Cloud/SaaS solution, the only on-premises components required are the log collectors (i.e. virtual collectors). For on-premises deployments the solution can currently use either an existing or a dedicated Splunk Enterprise deployment. Future plans cover the support of further platforms and the use of an integrated event