CRYPTOSIM

CYBER SECURITY INTELLIGENCE

- Log and Correlation Intelligence
- Security Risk Prioritization
- Incident Management over Any IT Enterprise
- Built-in Attack Patterns for Behavioral Inspection
- Security Information and Event Management

CRYPTTECH

CYBER SECURITY INTELLIGENCE

SECURITY INFORMATION & EVENT MANAGEMENT

With ever-growing IT groundwork in today's business world, monitoring and controlling event's track and providing security on networks are becoming more and more complex. Millions of log files are produced by devices and applications on an enterprise, containing crucial information and evidence for breach detection. Collecting and assessing these information in an integrated centralized platform, needs proper automated system. Although manual administration is necessary to deal with this complex task, automatedSecurity Information and Event Management Systems substantially help solving this problem to some extent. Log managers parse and collect logs and provide an actionable information to SIEM systems for security and compliance analysis.

CRYPTOSIM

CRYPTOSIM is a combined SIEM software with exceptional correlation and analysis features. It serves as a detection and controlling platform that can be deployed aligned with CRYPTOLOG.

CRYPTOLOG is a log management software to provide organization with threats detection and security risks evaluation on network behavior and performance.

CRYPTOSIM HIGHLIGHTS

- Threat detection and risk evaluation along with CRYPTOLOG
- Highly efficient correlation engines for event correlation from disparate parts and applications on the network
- Security incident prioritization and risk evaluation done based on real events correlations
- Incident management with alerts and real-time responses through instant command lines
- Numerous correlation types
- IP Reputation, GeoLocation, Malware/Phishing/Trojan services integration
- Efficient analysis on big data

CRYPTOSIM
CYBER SECURITY INTELLIGENCE

CRYPTTECH
CYBER SECURITY INTELLIGENCE

EVENT CORRELATION

Although log managers visualize the trend of actions on the network in one centralized interface, they usually provide basic contextual information on the events. Without a proper engine which correlates streams of events within a predefined interval, effective identification and response to breaches is not possible. Logs vary based on their source and operating system. That means, a firewall log may contain totally different information in comparison to the logs of the same event from other applications. With several advanced correlation rules, CRYPTOSIM not only discovers similar patterns of attacks among shreds of millions of event files, but also detects policy violations of any other mandates and validates the IDS and firewalls efficiency.

SIMPLE CORRELATION

It examines the correlation among logs of one resource.

LOGICAL CORRELATION

This correlation is based on assigning individual rules or events to correlation directives and applying logical trees to detect a misuse or attack over network.

CONTEXTUAL CORRELATION

This correlation is based on the known information on the asset value and types of targets and event reports. Based on the level of asset value, the likelihood of a security incident will be weighted and essential alerts will be produced.

RETROSPECTIVE CORRELATION

Besides real-time correlation on incoming logs, CRYPTOSIM can extract similar patterns from stored logs by correlating them with newly collected logs.

CROSS CORRELATION

CRYPTOSIM correlates logs of multiple devices and applications from various components of networks over the enterprise to verify the priority of incidents and events. In other words, logs of security vulnerabilities and Intrusion Detection Systems are correlated to substantiate an increase or decrease on the priority value of an incident.

HIERARCHICAL CORRELATION

CRYPTOSIM benefits administrators, with multi-level correlation by storing the correlated logs for further investigation. It re-correlates the stored logs with different rules and correlation engines to assess the priority value of an incident based on varieties of aspects.

CRYPTOSIM CYBER SECURITY INTELLIGENCE

CRYPTTECH CYBER SECURITY INTELLIGENCE

RISK EVALUATION & INCIDENT MANAGEMENT

CRYPTOSIM prioritizes security incidents and determines the risk percentage by utilizing state-of-the-art correlation engines to correlate event logs from all over the enterprise using several methods, from signature based anomaly detection and built-in attack patterns to behavioral inspection. Further to detection, it provides instant alerts and command line capabilities to administrators to respond in accordance with the detected incident.

SYSTEM REQUIREMENTS

SUPPORTED OPERATING SYSTEMS (BOTH 32-BIT AND 64-BIT)

- Windows 8,10,Server2008, 2012, 2016
- Ubuntu 12.04 LTS - Precise Pangolin
- Ubuntu 14.04 LTS - Trusty Tahr
- Ubuntu 16.04 LTS - Xenial Xerus
- Debian 6 , Debian 7, Debian 8
- OpenSuse 12.x, 13.2
- Red Hat Enterprise Linux 6.x, 7.3
- CentOS 6.x , 7.2
- Sun Solaris 10
- OpenSolaris 10.x, 11.x

VIRTUAL SYSTEMS

- Linux KVM-2.6.33 kernel version over (Kernel Virtual Machine)
- Citrix XEN Server 6
- Microsoft Hyper-V Server
- Free Xen Hypervisor 4.1, 4.0
- VMware vSphere Hypervisor 5.0
- VMware ESX & ESXi 4.x, 5.x, 6.x

EPS (MAX)	CPU	RAM	DISK
500	8 Core	16 GB	750 GB 7.2K RPM
1.000	16 Core	16 GB	1 TB 7.2K RPM
2.500	16 Core	24 GB	2 TB 7.2K RPM
5.000	24 Core	32 GB	5 TB 10K RPM
10.000	32 Core	64 GB	10 TB 15K RPM
25.000	64 Core	128 GB	20 TB 15K RPM

*: Calculated disk space for two year stored raw records and three months indexed data.

CRYPTOSIM
CYBER SECURITY INTELLIGENCE

CRYPTTECH
CYBER SECURITY INTELLIGENCE