Infopercept Proprietary Material

Security Information & Event Management (SIEM)

Technical - Approach
IT IS UNSAFE CYBER WORLD

ATTACKS TODAY -

OAS  ODS  NAV  WAV  IDS  VUL  KAS  BAD  RHK
IT Apps and Services are evolving

2006
Physical IT Service

2010
Virtualized IT Service
- Complexity Change volume,
- velocity

2016
Hybrid/Cloud Service
- Complexity Change volume,
- velocity Managed but not owned
Infopercept Vision for Security Operation Center
Vision for Security Operation Center

To provide business responsiveness, quality and cost advantages to customers’ IT Security operations to Global customers, through proven best practices and management solution globally accepted....
Need for SIEM Deployment
Why SIEM?

- Ability to Systematically Store and retrieve the logs for Compliance requirements.
- Drive collaboration between Operations Teams (NOC, SOC, Systems etc.) by providing
- Meaningful and Actionable information.
- Catch malicious activities delivered by exploit through Zero-Day-Attack.
- Cyber Forensic Investigations.
• Health check
  Support
  Assessment
• SIEM Design and
  Consulting
• SIEM Solution
  Selection and

Consult

• Data Source
  configuration
  and collection
  Architecture
• SIEM
  Implementation
• SIEM Upgrade
• Solution
  Integration

Integrate

• Use-Case
  Development
• Content
  Development
• Connector
  Development

Develop

• Use-Case
  Development
• Content
  Development
• Connector
  Development

Support

"Infopercept Proprietary Material - Please do not copy or distribute".
How Infopercept Builds SOC?
How we build SOC?

Infopercept builds a Security Operation Center which is a scalable and configurable suite of services to help you monitor all your IT elements more efficiently and costeffectively...
Elements of IT Environment

Hardware & Network
- Server
- Storage
- Desktops
- Network
- Printer

Software & Application
- Operating Systems
- Database
- Applications
- Email
- Patch Management
- Migration Services
- Deployment

Value Added Services
- Managed Security
- Help Desk
- Asset Management
- Risk Assessment
- Business Continuity
- L1, L2, L3 Support

*Infopercept Proprietary Material - Please do not copy or distribute*.
Infopercpect Delivery Model
SIEM Features and Value Proposition
Features of SIEM Implementation

**Anomaly Detection**
- DoS
- Recon
- Malware
- Suspicious activity
- User Access & Authentication
- Exploit
- Network
- Application
- Logins & Locations
- Administrative Accounts
- Infected Hosts detected on subnets

**Suspicious Activity**
- Traffic to known vulnerable host
- Logs deletion from Source
- Source Stopped Logging
- Various Protocol Traffic from unauthorized host

**Unauthorized Activity**
- User Access to confidential Data
- Subnet Access to Confidential Data
- Users on Network
- Devices on Network
- Server connection to Internet
SOC Model

Threat Connect

• Processes, analyze your data, and proactively hunt threats in one central place
• Aggregate and normalize threat data from any source
• View how often indicators are observed, how relevant they are

Splunk

• Collect and Index All Log Files Monitoring
• Forwards Data From Remote Systems
• Search and Investigate Across All Logs
• Real-Time Search

Infopercept Monitoring

• L1 Security Analyst
• L2 Security Analyst
• SOC Tech Leads
• SOC Managers
• Manage Security Solutions

"Infopercept Proprietary Material - Please do not copy or distribute"
Need for an IT Security

- Continuous monitoring
- Active scanning

Threat Monitoring & Intelligence
- Centralized Log collection – applications/devices
- Event correlation
- Incident response

Vulnerability Assessment

Protect Enterprise Data

SIEM
- Centralized Log collection – applications/devices
- Event correlation
- Incident response

Behavioural Monitoring
- IDS/IPS
- Monitoring – Apps, DB, Antivirus, Firewall/VPN, DLPs, Antispam, Web proxy etc.
- File Integrity monitoring

Continuous monitoring
- Active scanning
SIEM Systems require comparatively big investments. Organizations Management usually asks to seek value out of the tool from Information security team. The SIEM Use Cases are scenarios to detect a range of threat and deliver visibility you need to deal with it.

Understand Business Objective

Document Problem Statement

Define Use Cases

Generate Requirement Statements

Build Real Time Event Based Data Monitors

Create Content

Identify Data Sources

Prioritize Objective

Rules for Advance Corelation

Build Variables and Event Stream Analysis
USE Case – 1 (Malware Detection)

**Details**
The solution has detected traffic from `<source IP / hostname>` to `<destination IPs>` over `<ports>`. Information gathered would indicate the asset is infected with malware. Traffic activity is being reported by Suricata.

**Impact**
Malware is performing a remote call back, possibly leaking data or expanding its presence in the network.

**Description**
`<Detailed observations of the pattern and activity>`.

**Recommendation**
Find the source IP asset. Contain the device. If no signs of malware are found, determine the cause for the detected event and remediate. If signs of malware are found, perform the required antivirus updates and/or forensics on the machine. Remediate or clean the system prior to connecting it back on the network.
USE Case – 2 (Brute Force Attack Detection)

Details
The solution has detected failed login attempt from a source to multiple destinations over multiple ports. Information gathered would indicate the asset is infected with malware or an insider is conducting malicious activities. Activities are being reported by the Intrusion Prevention System (Suricata).

Impact
A malware or an insider is trying to gain access to resources by using brute force attack.

Description
Detailed observations of the pattern and activity.

Recommendation
Find the source IP asset. Contain the device. If no signs of malware are found, determine the cause for the detected event and remediate. If signs of malware are found, perform the required antivirus updates and/or forensics on the machine. Remediate or clean the system prior to connecting it back on the network.
USE Case – 3 (Privilege Escalation)

Details
User is added to a privileged access group at non working hours.

Impact
An insider has added a new user to privileged access group to access resources which are not intended for them.

Description
<Detailed observations of the pattern and activity>.

Recommendation
Check with Identity Management team to verify the authenticity of user addition to privileged access group. If it's unauthorized, take the remediation actions.
USE Case – 4 (Network Scan Detection)

Details
Intrusion Prevention System (Suricata) has detected probes from a source on various destination which hosts business critical applications.

Impact
It might be possible that an intentional intruder is trying to perform a network scan on random hosts for recon.

Description
Detailed observations of the pattern and activity.

Recommendation
Report to network management team to verify the incident and take remediation action.
TEAM @ Infopercept

Operating System
- Windows
- Solaris
- HP-UX
- AIX
- Linux

Database
- MS SQL
- MySQL
- Oracle
- Sybase
- MariaDB

Messaging
- MS Exchange
- Lotus
- Domino
- Zimbra

Web / App. Servers
- IIS
- Tomcat
- Apache
- WebLogic
- WebSphere

Process Certification
- ITIL
- SIX Sigma

Security Certification
- CISSP
- CISA
- BS7799 Auditors

Database Certification
- OCP
- OCA
- MCDBA

System Certification
- RHCE
- SCSA
- SCNA
- MCSE
- MCSD

Service Tools

Network Certification
- CCNA
- CCNP
- CCIE

Best of breed best of exposure

"Infopercept Proprietary Material - Please do not copy or distribute"
About Infopercept

Infopercept’s vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners’ cybersecurity and accreditation needs.

Our specialized core team comprises of experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, are abreast of the latest trends and security innovations; ensuring that you always get the best security approach & solutions for your specific business needs, exactly the way you want it to be.