BUILDING AND MAINTAINING SOC

Digit Oktavianto

KOMINFO

7 December 2016

digit dot oktavianto at gmail dot com

Profile in 1 Page ☺

Currently working as a Security Architect

Professional Certifications:

- Certified Ethical Hacker, EC Council
- GIAC Certified Incident Handler (GCIH)
- IBM Qradar Security Analyst

Specialization and Interest :

- Cyber Security Operation Center
- Threat Hunting
- DFIR
- Malware Analysis
- Cyber Defense Operation
- Threat Intelligence
- OSINT
- Incident Handling and Incident Response
- Active Defense and Continuous Monitoring

More than 5 years in **Information Security Field**

SECURITY OPERATION CENTER

Organization faces many challenges in protecting its data and IT infrastructure. Organization is experiencing compromises on a daily basis. The threats are real and increasing, and now include sophisticated Advanced Persistent Threats.

- A security operations center provides centralized and consolidated cyber security incident prevention, detection and response capabilities.
- Security operations functions :
  - Security monitoring
  - Cyber security incident response management
  - Threat and vulnerability management
  - Security device management and maintenance

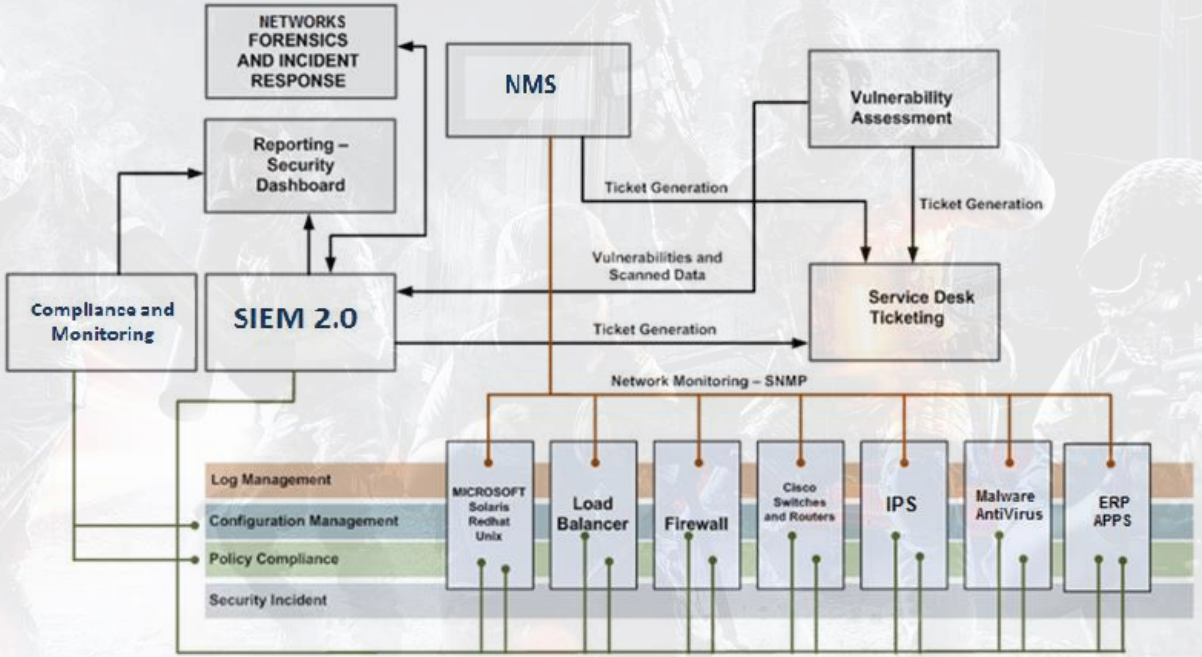
WHY NEED SOC

- Because a firewall and IDS are not enough
- Center of all information security operations
- It provides :
  - Continuous Monitoring
  - Detection
  - Protection and Prevention
  - Response capabilities against threats, remotely exploitable vulnerabilities and real-time incidents on the networks
- Works with CERT (Computer Emergency Response Team) / IR Team to create comprehensive infrastructure for managing security operations

CYBER SECURITY MONITORING AND INCIDENT MANAGEMENT

Implementing a cyber security incident management capability in practice

CORE COMPONENT TECHNOLOGY



So, If I Buy All of the Technologies, will I have a SOC?

BIG NO !!!!!!!!!!

SOC involves PEOPLE and PROCESS which are in fact MORE IMPORTANT than tools

BENEFIT OF HAVING SOC

- Security Operation Center can satisfy compliance regulatory and enhance security capability for organization. These can range from self-service solutions that require clients to view their own incident alerts in a portal to full-service solutions that will proactively alert clients when security incidents occur. Benefits of partnering with an MSSP for maintaining Security Operation Center are :
  - Access to security expertise, research and threat intelligence.
  - Efficient process, procedure, and workflow to improve time in remediation and mitigation security issues.
  - Saving time on building team and setup infrastructure for developing proper SOC
  - Cross-device and cross-vendor correlation to improve security awareness and reduce risk.

SOC EXPECTATIONS :

- Watch and protect the infrastructure
- Monitor Network Traffic, watching for anomalies
- Protect Users
- Internal and External Threat detection
- Alert and Escalate
- Internal and External Threat mitigation

SOC EXPECTATIONS :

….and also

- Monitor Users
- Systems Configuration
- Data Loss Prevention
- Forensics Analysis
- Threat modeling

SOC MISSION

1. Prevention.
2. Monitoring, detection, and analysis.
3. Response and Mitigation
4. Providing situational awareness and reporting.
5. Engineering and operating CND technologies.

MISSIONS #1

Prevention of cybersecurity incidents through proactive:

- Continuous threat analysis
  - SIM + SEM = SIEM
- Network and host scanning for vulnerabilities
  - Vulnerability Management.
- Countermeasure deployment coordination
  - NIPS & HIPS
  - AV / NGAV
  - Endpoint Detection & Response
  - WAF
  - BDS (breach detection systems) + SWG (proxy)
  - NGFW / UTM
- Security policy and architecture consulting.
  - 3rd party engangement

MISSIONS #2

Monitoring, detection, and analysis of potential intrusions in real time and through historical trending on security-relevant data sources

- SIEM
  - Near Real Time (there must be a delay).
  - Correlation & Rule based.
- Security Analytics (threat hunting)
  - Finding needle in a stack of needles (security big data)
  - Historical

MISSIONS #3

Response by coordinating resources and directing use of timely and appropriate countermeasures. Usually referred as incident handling & response.

- Quarantine (damage control)
  - Block Activity.
  - Deactivate Account.
- Remediate.
  - Re-image.
  - Virus scan
- Continue Watching.
- Refer to Outside Party.
  - Browse
  - Phone a friend

MISSIONS #4

Providing situational awareness and reporting on cybersecurity status, incidents, and trends in adversary behavior to appropriate organizations

MISSIONS #5

Engineering and operating CND technologies

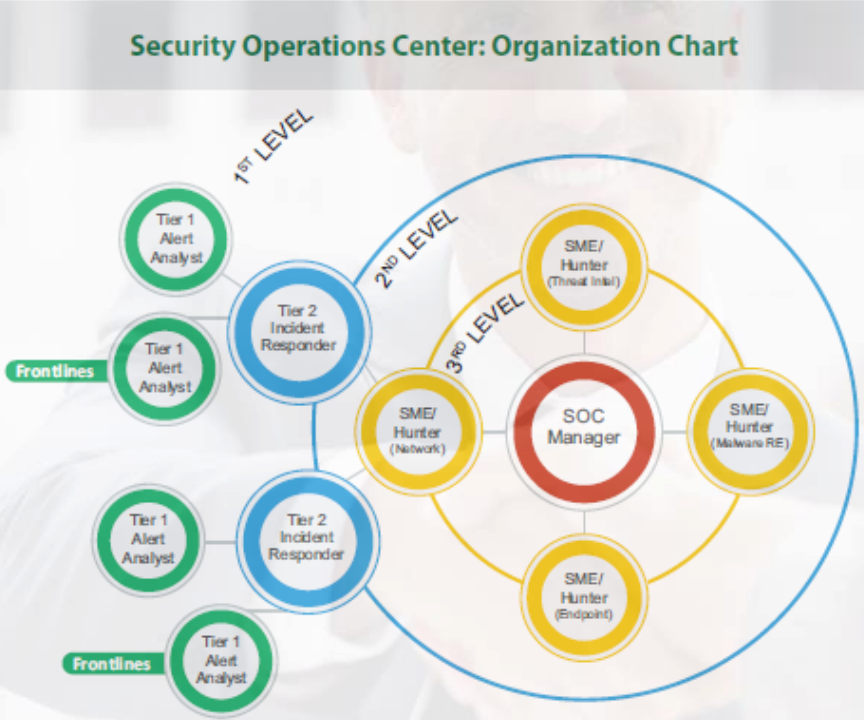
- FW
- Endpoint Protection
- IPS
- BDS (Breach Detection System)
- Secure Web Gateway
- Email Security
- SIEM
- Packet Sniffer
- Security Analytics

SOC BUILDING BLOCKS

Triad of Security Operations: People, Process and Technology

PEOPLE

- SOC Organization Chart

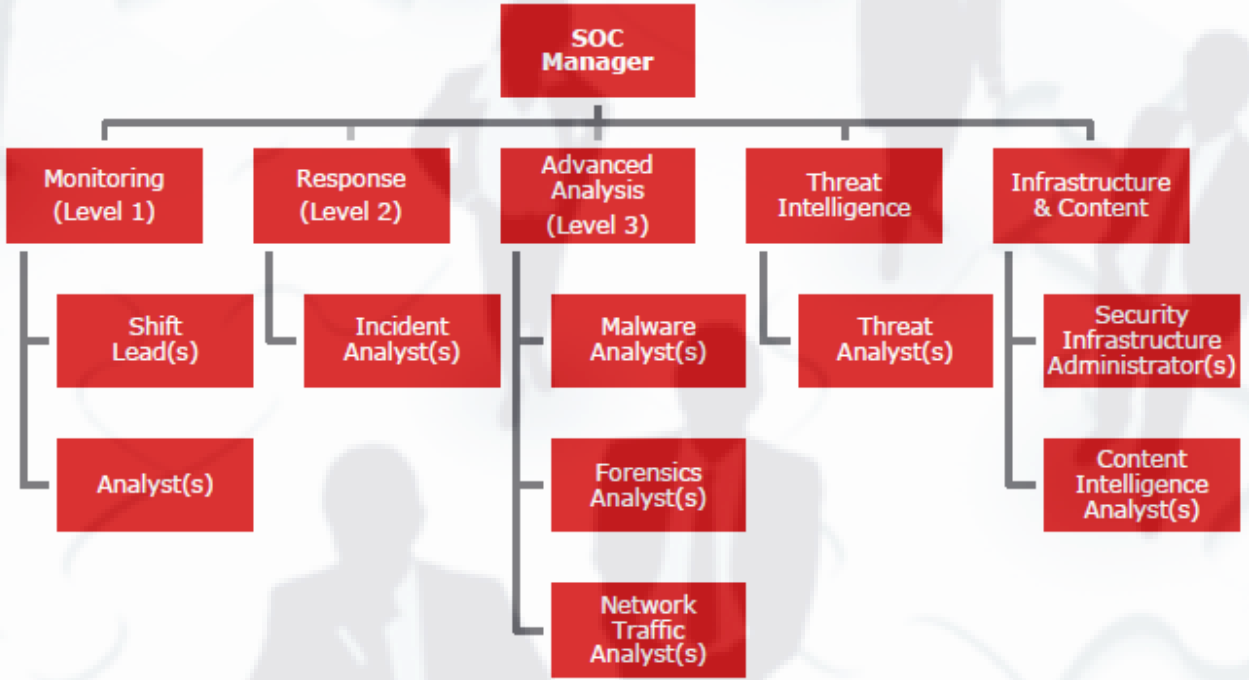


PEOPLE

SOC Organization Chart :

- SOC Manager
- SOC Analyst
  - Level 1
  - Level 2
- Incident Handler / Responder
- Forensic
- Malware Analyst
- Threat Hunter

SOC ORGANIZATION BEST PRACTICE



PROCESS

SOC processes are broken up into the four main categories :

- Business processes : Document all the administrative and management components that are required to effectively operate a SOC.
- Technology processes : Maintain all the information relating to system administration, configuration management and conceptual design.
- Operational processes : Document the mechanics of the daily operations, like shift schedules and turn-over procedures.
- Analytical processes : Encompass all activities designed to detect and better understand malicious events.

PROCESS

- Define Business Process Procedure
  - SOP for Incident Handling
- Define Technology Process
  - SOP for Changes Management
  - SOP for Problem Management (troubleshooting)
  - SOP for Deployment SIEM

PROCESS

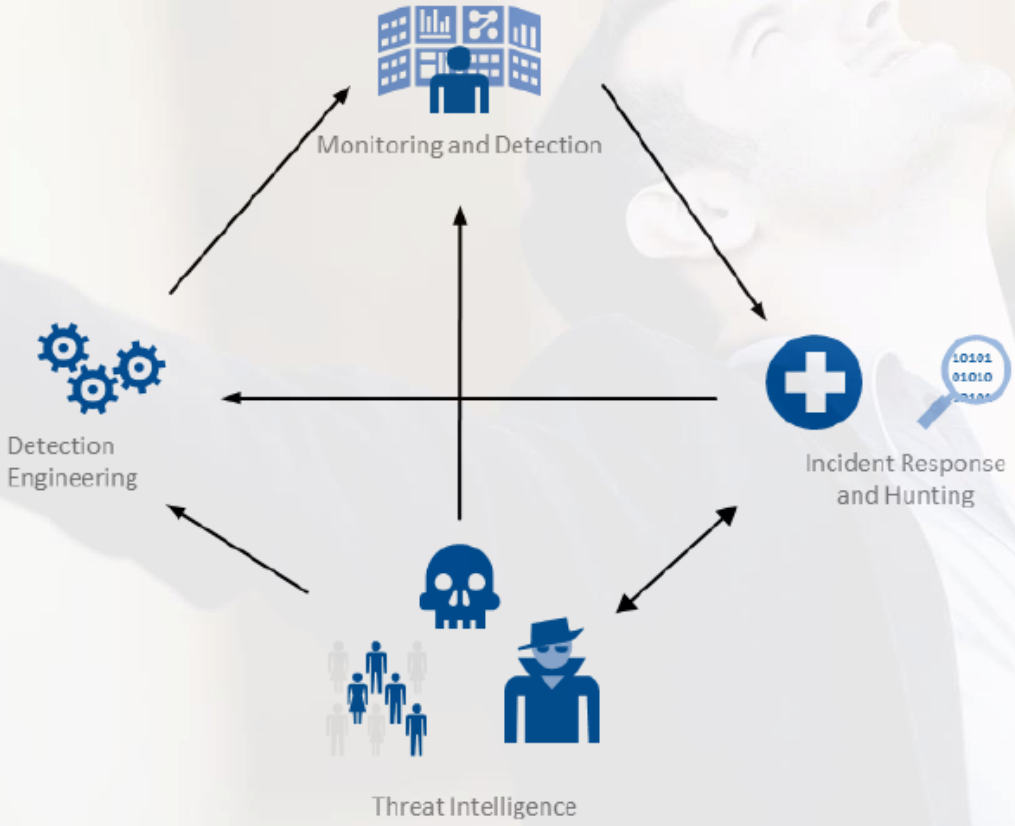
- Define Operational Process
  - Shift Staff Schedule
  - Personnel Shift Reporting
  - SLA for Incident Response
  - SLA for recommendation and solution for security threat ticket
- Defining Analytical Process
  - SOC Workflow (Ticketing, Analysis Security Events, Escalation, Response, etc)
  - Security Incident Procedure Flow
  - Reporting Document for Customer

TECHNOLOGY

Modern SOC Tools

- SOC “Weapon Triad”
  - LOGS: Log analysis -SIEM
  - NETWORK: Network traffic analysis (NTA and/or NFT)
  - ENDPOINT: Endpoint activity analysis –EDR
- Analytics
  - UEBA / UBA (User Behavior Analysis) and other security analytics
- Threat intelligence
- Incident Respond and Forensic Tools

MODERN SOC MODEL?



FAMILY OF SOC SERVICES

❖Select SOC own processes:

1. Alert triage
2. Use case content management / detection engineering
3. Threat hunting

❖Select SOC process dependencies:

1. Security incident response
2. IT Change management
3. IT Asset management

MAINTAINING SOC

- Staff Schedule
- Transfer / Update Knowledge
- Lab Exercise and Use Case
- Expanding / Upgrading Technology

SOC USE CASE

Use Case	Primary Data Sources	Alert Criteria	Action
Botnet activity	Firewall, IDS, Proxy, Mail, Threat Intelligence	Connection to or from known malicious host or domain	Display in analyst active channel
Virus outbreak	Antivirus	3 viruses detected with same name in 10 minutes	Page desktop team / display in dashboard
Successful attack / malicious code	IDS/IPS, Vulnerability	Targeted asset exhibits vulnerability, relevance=10	Page server team / display in active channel / display in dashboard
SQL injection	Web Server, DAM, IDS/IPS	5 injection attempts within specified time frame	Display in analyst active channel
Phishing	Threat Intelligence, Firewall, IDS, Proxy, Mail	Connection to or from known malicious host or domain	Display in analyst active channel
Unauthorized remote access	VPN, Applications	Successful VPN authentication from a non domain member	Display in analyst active channel / Page network team
New vulnerability on DMZ host	Vulnerability	New vulnerability identified on publicly accessible host	Email daily report to vulnerability team
Suspicious activity	Firewall, IDS, Mail, Proxy, VPN	Escalating watch lists (recon, exploit, brute force, etc.)	Email daily suspicious user activity report to level 1
Statistical anomaly	IDS, Firewall, Proxy, Mail, VPN, Web Server	Moving average variation of X magnitude in specified time frame	Display alerts in situational awareness dashboard
New pattern of activity	IDS, Firewall, Proxy, Mail, VPN, Web Server	Previously unseen pattern detected	Display in analyst active channel

SOC CHALLENGES

- Trying to build a SOC with limited resources (people, tools, budget)
- Sole focus on alert pipeline; no deeper analysis apart from “processing” alerts that are shown to analysts
- Not enough visibility tools; sole focus on SIEM
- Vendor dependencies (Especially the Core System : SIEM)
- Trying to provide SOC services from a NOC/Help Desk
  - Different Point of View / Mindset from NOC to SOC
- Not working to retain staff and not having a staff retention strategy

SOC CHALLENGES

- Most of SOC in Indonesia still adopt REACTIVE Approach instead of PROACTIVE Approach (Threat Hunting and Threat Intelligence)
- SOC Needs visibility down to the Host Level (Endpoint)


host-based
Authorized
Red
Protocols
threat
Capability
service
Software
Boundary
Fill
file
Data
DLP
Malware
Continuous
Need
behavioral
Unauthorized
Administrative
Engineering
Network
Training
Servers
Appropriate
Routers
Exercises
security
integrity
intelligence
Security
Recovery
HIDS
Configurations
Vulnerability
intrusion
Control
Tests
Based
discovery
Defenses
Workstations
Penetration
Loss
Inventory
Skills
Monitoring
Application
Access
Know
Controlled
Firewall
passive
Ports
monitoring
network
Limitation
Anti-Virus
Maintenance
Analysis
wireless
detection
Prevention
Account
Assessment
Laptops
Firewalls
Team
Use
Switches
Wireless
Hardware
flow
assessment
active
Remediation
inventory
Gaps
Secure
Response
Incident
Logs
Device
Audit
asset
SIEM
Privileges
scanning
Services
Devices
vulnerability
Defense
WIDS
IDS


FINISH
Q &A