

## How to build and run a Security Operations Center

v1.1

**Nicolas FISCHBACH**

Senior Manager, Network Engineering Security, COLT Telecom  
nico@securite.org - <http://www.securite.org/nico/>

# About

- Nicolas Fischbach
- Head of Technology Security at COLT
  - Tier-1 SP in EU, data/voice/managed services
  - 13 countries, going NGN, expanding reach
- Recognized Service Provider security architect
- Member of the HoneyNet Project
- Teacher (university and engineering schools)
- Frequent speaker and writer

# Agenda

- Introduction : Why build a SOC
- Non-technical requirements
- Technical requirements
- Technology deployment
- Processes, procedures and KPI
- Challenges
- Conclusion



# Intro :: SecOps as we know it

- Usually non-existing
- Often a side-job (engineering group)
- Limited FTEs (less than half a dozen)
- No proper separation of duty
- Lack of change management
- Reactive security
- etc...

# Intro :: Various groups

- SOC
- CERT
- CSIRT (Company/Computer/Corporate)
- PSIRT (Product)
- Internal audit / Legal&Regulatory / Safety
- C(I)SO organization
- Where do you put the SOC and is it really a SOC you are looking for ?

# Intro :: Duties of a SOC

- Define the duties of your SOC
  - Internal security devices management
  - External security devices management
  - Managed customer services
  - Proactive/reactive incident handling
  - Security event management
  - Forensics
  - Vulnerability management
  - Audit/Pen-test



# Intro :: Optional duties ?

- Technical Infrastructure
  - Badge systems / CCTV
- Facilities Management
  - Fire alarms, building management systems
- Physical security teams
- (S)PoC for Business Continuity and/or Disaster Recovery
- Law Enforcement Agencies interface
  - Data Retention, Lawful Intercept, etc.



# Non-tech :: The SOC in the ORG

- Separation of duty with IT, Network Ops, Engineering, etc.
- Where is it to be attached ? Eng, Ops, C(I)SO, Audit ?
- Integrated/outside helpdesk
- 1st/2nd/3rd level and vendor escalation ?
- Vendor management (vs Eng/Procurement)
- Who “watches” the SOC

# Non-tech :: SOC P&Ps

- Define clear operations
  - Procedures
  - Processes
  - Policies
- Ticket management system
- Authorization system
- Authentication of incoming requests
- Bureaucracy vs flexibility
- SOC handbook (count 1+ year)



# Non-tech :: SOC SLAs and KPIs

- Which KPIs and SLAs make sense
- You can't really measure on failure
- You can't really measure on volume
- What is "a change" ?
- What are realistic SLAs for changes
- What are realistic SLAs for TTR



# Non-tech :: Setting priorities

- What needs to be dealt with ?
  - In near real-time (NRT)
  - Next business day(s)
  - Long term
- What triggers it ?
  - Security events
  - Change requests / TTs
  - Forensics / event analysis
  - Law enforcement



# Non-tech :: Basic requirements

- Is your SOC 24x7 ?
- Follow the sun approach
- How many FTEs do you need
  - -20% due to leaves/trainings/sickness
  - 9 FTEs is a minimum for a basic 24x7 SOC
- What are the legal requirements
  - Data protection
  - Security clearances (and background checks)



# Tech :: SOC PHY architecture

- Separate network(s)
- Heavily filtered / dedicated non-Internet connected network
- How to interface with customers (“secure” channel) for requests
- How to interface with customers networks/devices (management and monitoring) ?



# Tech :: SOC OSS architecture

- Should all the systems be contained inside the SOC ?
- Management platforms
- Monitoring platforms
- AAA systems
- Secure storage and backup
  - Data may be used in court
  - Chain of custody



# Tech :: SOC Dashboard

- For you or for management ? :)
- SEM (Security Event management)
- Data visualization
- What do you want to measure, display, act on, report on, etc ?
  - MSSP-only ?
  - Internal and Internet facing systems ?
- Internal knowledge base

# Tech :: External interfaces

- Network Operations / IT Operations
- Third parties
- Customers
- Often no clear demarcation between network and security especially on complex devices
- Integrated or separated test lab ?



# Tech :: Data feeds

- You'll be flooded with data. Do you really need more ?
- Commercial data feeds
- Public data feeds
- Vulnerability analysis data



# Ops :: Data Visualization

- You will have \*LOTS\* of data
- Parsers are helpful
- Visualization is key
- Pick the right tool
- Write the right rules
- Have enough displays



# Ops :: Keeping the SOC secure

- Physical access
- Logical access
- Keep the networks REALLY separated
- Hardened clients and servers
- Intrusion detection in the SOC
- Patch management, vulnerability management, etc.
- Dedicated system/network ops within the SOC?



# Challenges

- Humans
- Processes and procedures
- Legacy
- Technology
- Noise



# Challenges :: Humans

- Finding the right people
- Skills
- 24x7
- Language
- Background checks / Security clearance
- Keeping these guys motivated
  - Security analyst, incident manager, administrative contact, hard core geek

# Challenges :: P&Ps

- Key procedures
- Key processes
- Bureaucracy vs flexibility
- Integration with the
  - Ticketing system
  - Request system



# Challenges :: Legacy

- Green field approach
- How much legacy ?
  - Technologies / vendors
  - EoS/EoL
  - Undocumented configurations / setups
  - People



# Challenges :: Noise

- How do you deal with the noise ?
- Internet background noise
  - Scans and SPAM
  - Dark IPs and Netflow
  - Honeypots
- Customer generated noise
  - ACLs/Security policies with logging
  - IDS systems
  - Anti{-virus, -malware, etc}

# Challenges :: Technology

- Which technology can you decide on ?
- Which technology is “forced” on you by Marketing and Sales
- How to pick
  - The right AAA system
  - The right SEM platform
  - The right management and monitoring platform



# Challenges :: Technical

- How to run your own OSS/NMS/IS inside the SOC ?
- How to get stable and secure remote connectivity into all the devices you need to manage
- Separated networks and their limitations (Internet vs secure)
- Fine-tuning of systems (esp. a SEM) takes at least a year



# Challenges :: SEM/SIM

- A challenge of his own
- Events/second driven
- Database structure and storage size
- Rules/"AI"/"NNs"/marketing
- Log parsers, input modules, etc.
- Do you have development people inside a SOC?
- More complex and time consuming than OSS/NMS



# Conclusion

- Building a SOC is complex
- Pick the right technology, team and P&Ps
- Maintaining a SOC in the long run is even more a challenge
- Remember
  - 1) It's all about people
  - 2) It's all about having the right technology in place
  - 3) It's all about trying to make the 3Ps work by finding the right mix of flexibility and bureaucracy