

Come rilevare un incidente di sicurezza: il Security Operation Center (SOC)

Esperienza di implementazione in una
azienda multinazionale

Group Information security master plan 2017 – 2019 Budget

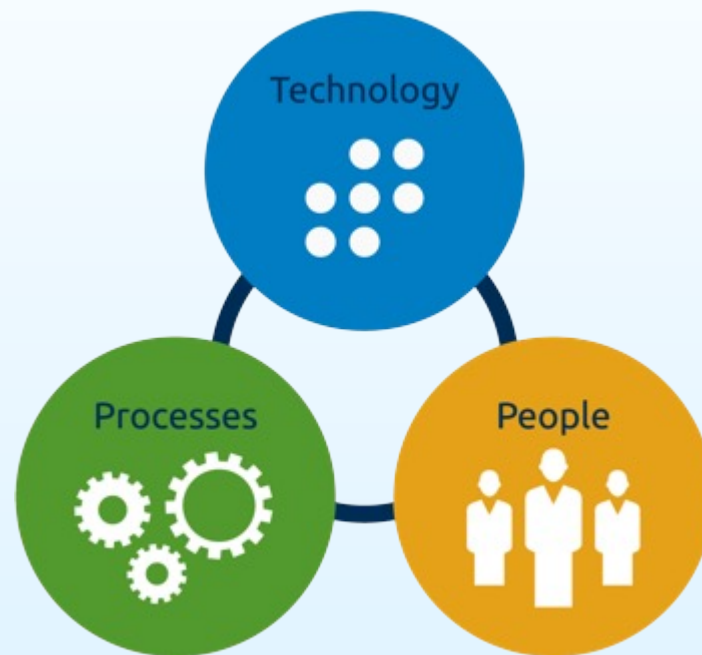
Capability Domain	Macro-Initiatives	Objective	2017 (K€)		2018 (K€)		2019 (K€)	
			Inf. Sec.	IT Security	Inf. Sec.	IT Security	Inf. Sec.	IT Security
Governance	G.1 - Information security steering improvement	Ensure clear strategic direction on information security at group level through a clear and effective organization, policies, risk management process and vendor management						
	G.2 - Information security competencies & monitoring capabilities improvement	Develop adequate information security capabilities as well as monitoring at group level						
Prevent	P.1 - Data protection enhancement	Protect most critical Company's information during their entire lifecycle						
	P.2 - Access and authentication improvement	Ensure an effective management of identities and access to critical company data and critical operations						
	P.3 - Applications Security Improvement	Ensure a secure development of applications as well as improve security of the critical ones						
	P.4 - Infrastructure Security improvement	Improve protection against malware, unauthorized access, misuse or modification of network-accessible resources.						
Detection & Response	D.1 – Security Operation Center Implementation	Ensure the effective detection and analysis of security events, an adequate response to them						
	D.2 – Crisis & Continuity Improvement	Ensure the recovery after major security incidents						
	D.3 – Threat Management Improvement	Ensure the effective management of cyber threats as part of the wider monitoring and incident detection / brand protection processes						



Security Information and Event Management

Desired Target:

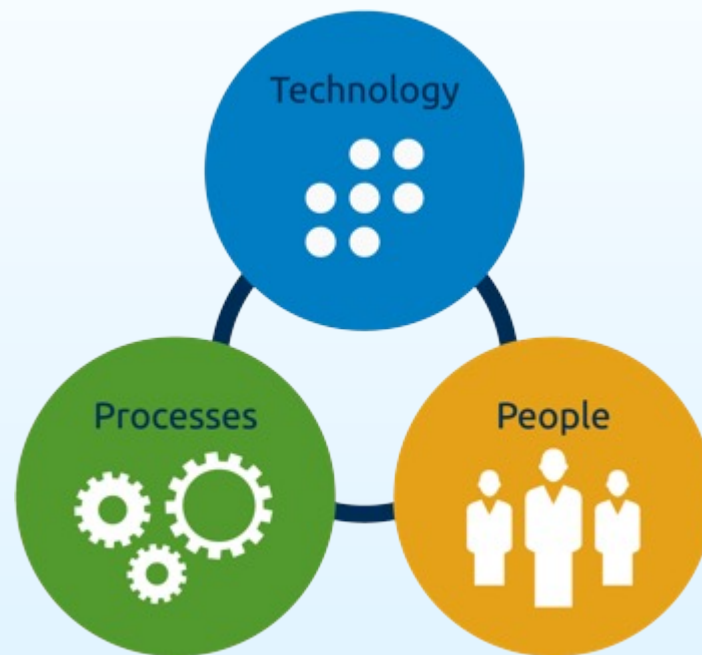
- SIEM Tool Selection Options:
 - Splunk
 - HP – ArcSight
 - IBM – Qradar
 - Logrhythm
- Proper SIEM tool selection
 - Must be a globally scalable solution
 - Must be able to deliver in first year
 - Must support cloud operations as well as on premise
 - Must be able to provide real time alerting
 - Must be able to be supported by internal, and also by a MSS if desired
- Solution must be flexible to accommodate the Company diversified administrative model, and work with the future incident response process.



Security Operation Center







Consideration

- Technology (Tools)
 - Utilizing existing Splunk structure as SIEM, expand as necessary,
 - Evaluate Cloud as possible Hybrid Solution for Splunk, quicker to stand up
 - Review internal tools
- People
 - Vendor MSS
 - Leverage vendor resources (tools / staff / knowledge) to cover key Group locations
 - Staffing:
 - Use North America IT Security as initial COE – leverage existing staff, tools, approach to initiate SOC
 - Leverage vendor staff to follow the sun
 - Vendor needs to offer more than just staff augmentation –
 - must aide in identification, escalation and remediation activities to be effective (part of incident management not just ticketing approach)
- Processes
 - Develop policies, processes and observe impact
 - Evaluate over time how COE should be managed in a more mature environment
 - Approach would balance internal and external expertise to achieve SOC Model goals



A SOC can perform an extensive set of security services – the core part is the incident handling

Core / Primary Services of a SOC

	Security Incident Handling 	Proactive Security 	Security Management 
 Monitoring	<ul style="list-style-type: none"> • Sec. Incident Detection ● • Sec. Incident Classification ● 	<ul style="list-style-type: none"> • Real Time Device Monitoring ● • Vulnerability Assessment ● • Penetration Test ● • Security Audit ● • Security Intelligence ● • Performance Monitoring ● • Fault Monitoring ● • Policy Compliance ● 	<ul style="list-style-type: none"> • Business Impact Analysis ● • Risk Assessment ● • Technology Watch ●
 Advising	<ul style="list-style-type: none"> • Sec. Incident Notification ● 	<ul style="list-style-type: none"> • Alerting & Warning ● • Technical Reporting ● • Security Hotline ● 	<ul style="list-style-type: none"> • Executive Reporting ● • Security Consulting ● • Awareness ● • Countermeasure Selection ●
 Managing	<ul style="list-style-type: none"> • Sec. Incident Response & Containment ● • Sec. Incident Recovery ● • Forensics Evidence Collection ● • Tracking & Tracing ● 	<ul style="list-style-type: none"> • Security Device Configuration ● • Security Device Maintenance ● • Policy Management ● • Policy Enforcement ● • Security Patch Management ● • Endpoint Management ● • Hardening ● 	<ul style="list-style-type: none"> • Business Continuity ● • Asset Inventory ● • Risk Management ● • Education/Training ● • Certification ●

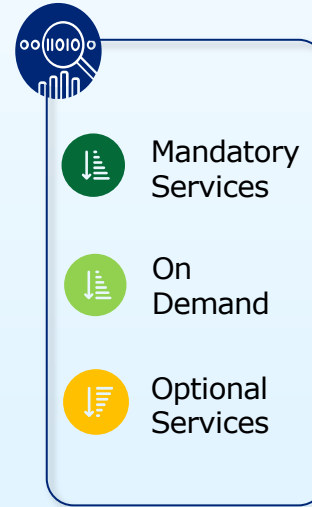
Please note that management of traditional IT Incidents (not Security related – e.g. Computing / Disk Resource Constraints or Failure, Network Issues, Application Bugs, etc.) are not in scope of SOC perimeter

● Mature capability ● Capability to be improved ● Not performed

We are looking for a vendor to help us in:

Services in Scope of RFP

- SIEM¹ Operation & Management;
- Security Incident Detection, Classification and Notification (24X7;)
- SIEM Customization Services;
- Security Incident Response;
- Security Incident Investigation;
- Threat Intelligence;
- Vulnerability Assessment;
- Installation, Operation & Management of IDS/IPS²;
- Integration Services;

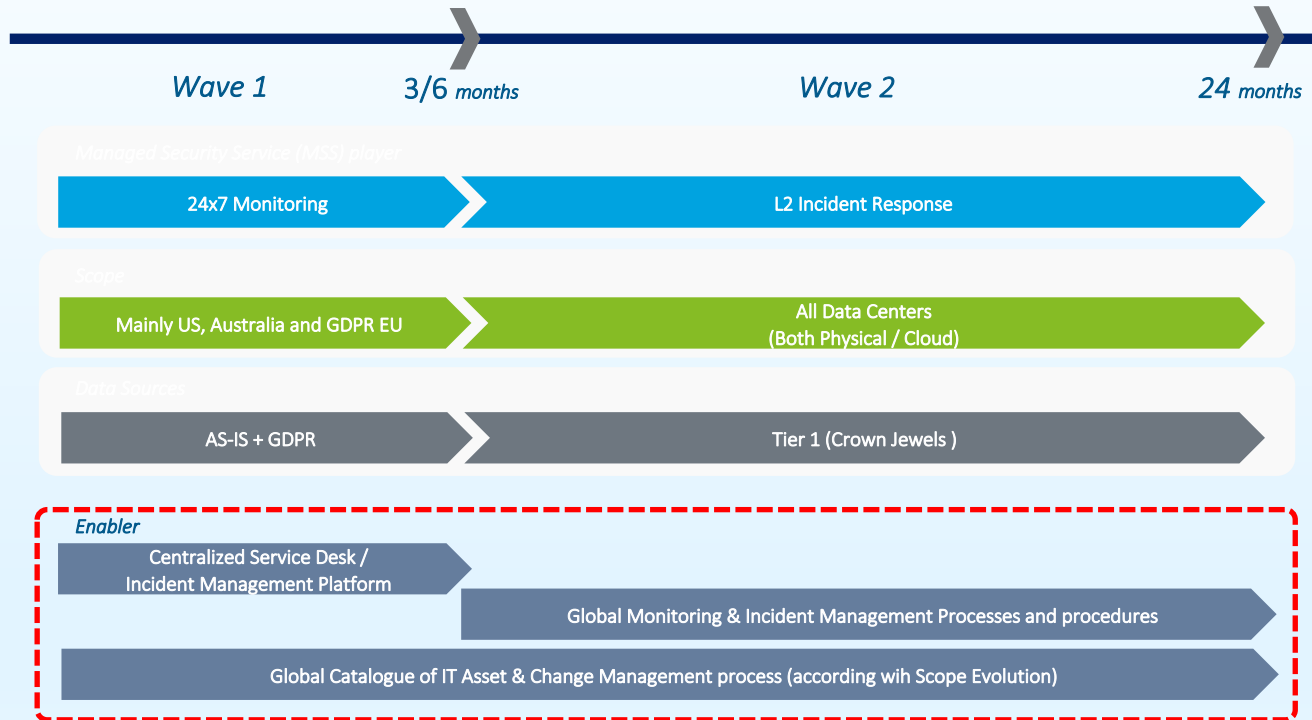


¹SIEM: security information and event management

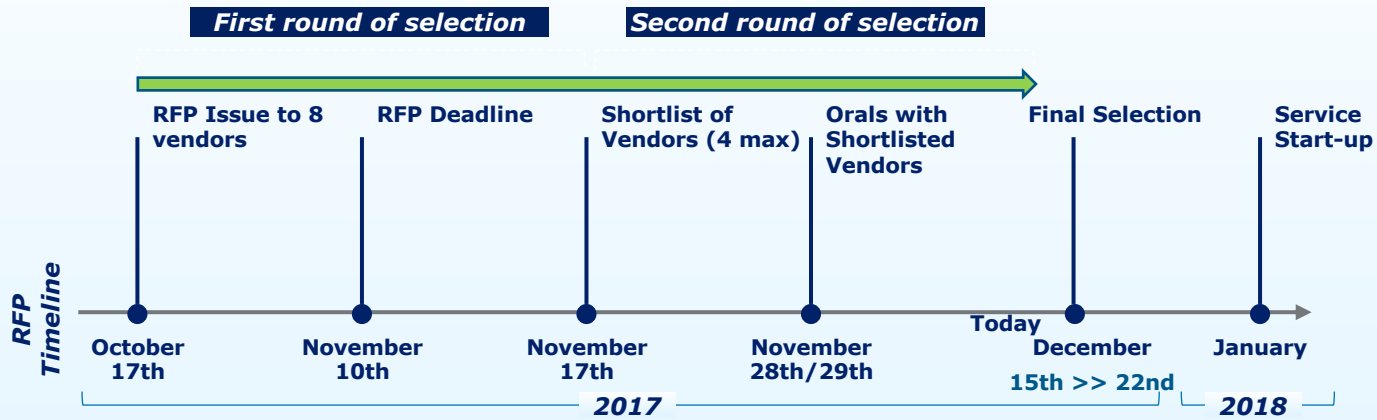
²IDS/IPS: Intrusion Detection & Prevention Systems

POSSIBLE TIMELINE IMPLEMENTATION:

Build a 24/7 monitoring and incident response process while growing Company SIEM capabilities



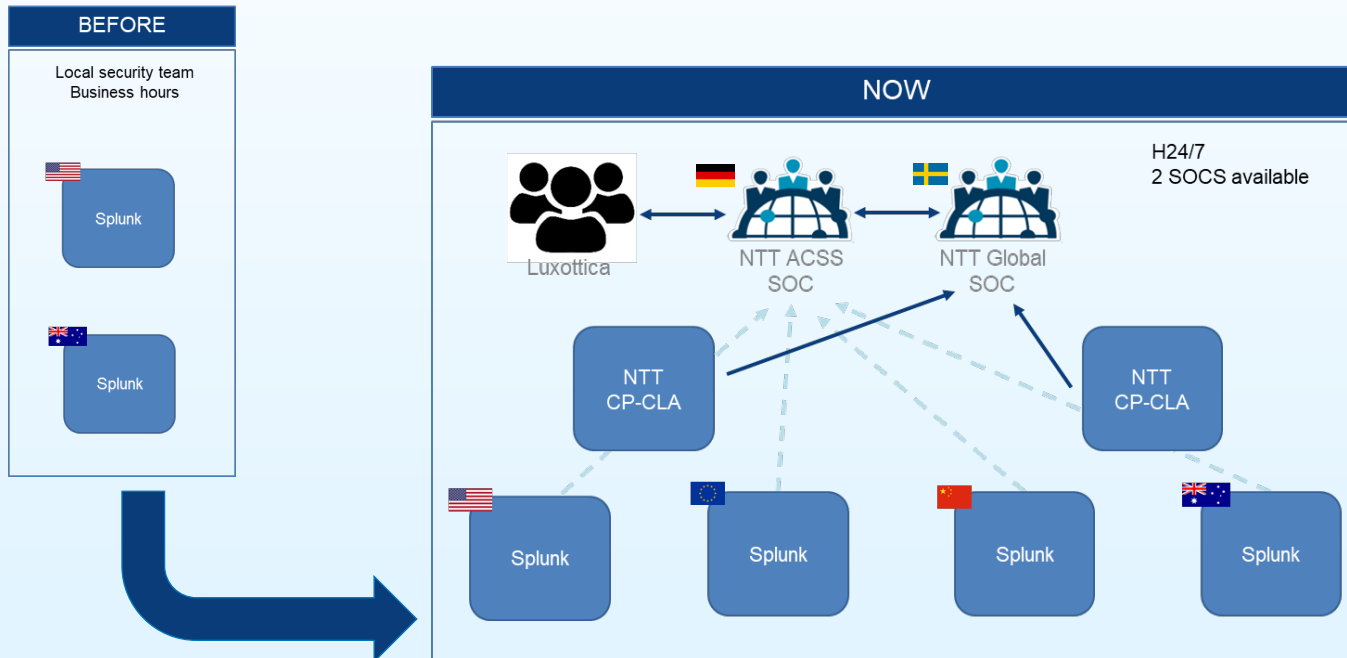
It has been issued an rfp organized according to a two round process - the economic effort for will be significant



Invited Vendors

- AT&T
- Capgemini
- Symantec (Sinergy presented the tender)
- FireEye
- Leonardo
- Deloitte
- Binary Defense (TRUSTEDSEC, LLC)
- DELL as SecureWorks
- NTT

OVERALL ARCHITECTURE



SECURITY OPERATION CENTER

In a world of new technology based on growing importance of data and data processing, Company decided to establish a SOC as center to manage, control and proactively monitor security in a centralized and global manner



Done

- Manage Splunk Data standardized over 4 regions
- Establish Global Threat Detection
- SOC service to identify and analyze critical incidents
- Incident Response global process
- Alignment weekly call
- Acceleration workshops (Agordo and two in Mason)
- Cyber-Defense-Platform to handle security cases
- Activated base ticketing portal (based on RSA Archer) for tracking incidents



In progress

- GDPR use-cases and device integration
- Integrated incident management process (ref ServiceNow initiative)
- GDPR Dashboard
- China under deploy stage
- Logs forwarding for critical environments



To be done

- Global Incident Response workshop
- Splunk version up-grade
- Splunk use cases extension
- Collect via ATP the alerts to improve the remediation

Grazie