Answers on security center establishment process

- Reliable partner for today and tomorrow

Terminology

Network Operating Center (NOC) - A network operations center (NOC) is a place from which administrators supervise, monitor and maintain a telecommunications network. The network operations center is the focal point for network troubleshooting, software distribution and updating, router and domain name management, performance monitoring, and coordination with affiliated networks.

Security Operations Center (**SOC**) is a centralized unit that deals with security issues on an organizational and technical level.

Computer emergency response team (CERT) or Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity.

Differences between SOC and CERT

Organization type	Goal	Responsibilities	When to Create
SOC	is to implement and oversee network, application, cloud, and user security, among other operational functions. SOC is created mostly on business enterprise level in case of single tenant organizations.	1. Executing against the overall company security strategy under the head of security Overseeing the security of systems, applications, and users 2. Integrating security systems with other operational tools 3. Preventing, detecting, and responding to ongoing security threats 4. Governance, risk, and compliance 5. Policy and procedure creation and management	1. Your organization is handling increasing amounts of sensitive data 2. Your emerging threat landscape requires dedicated security resources 3. Your organization is growing 4. There are no standard processes, procedures, or ownership over security 5. It's difficult to measure the ROI on security spend because security is a part of another function (e.g. IT) 6. You need improved monitoring and response capabilities 7. You've outgrown your managed security service provider (MSSP)
CERT	The ultimate goal of a CERT is to minimize and control the damage resulting from an incident, which is why so many different functions can be involved in some capacity. You need to not only address the threat itself, but also communicate to customers, your board, and the public about the incident. If a malicious internal actor caused the event, disciplinary, and perhaps legal action will need to be taken on involved employees. Mostly CERT is created on government level or in case of multinational organizations.	1. Preventing, detecting, and responding to ongoing security threats 2. Ranking and escalating alerts and tasks 3. Investigating, analyzing, and conducting deeper forensics on incidents 4. Developing communication plans (for public relations, customers, board members, etc.) 5. Coordinating and executing response strategies 6. Maintaining a repository of log data related to events for future reference, as well as for compliance or legal purposes 7. Education and increasing security awareness	The CERT may be a formal or informal organization, depending organizational unique needs. If you're not faced with threats on a regular basis, the CERT may come together only on an as-needed basis. But if you're in a high-risk industry (e.g. government, healthcare, finance) where responding to threats is a regular and vital part of your business strategy, a formal and full-time CERT may be necessary. Your CERT may evolve over time, too. While it may start off as an informal team that gathers on an as-needed basis, it may develop into a full-on function if incident response needs necessitate it.

Law enforcement for incident interchange in Serbia

Law on information security

Decision on Minimum Information System Management Standards for Financial Institutions

Security center creation process

EDUCATING STAKEHOLDERS ABOUT THE DEVELOPMENT OF A NECESSARY SECURITY TEAM

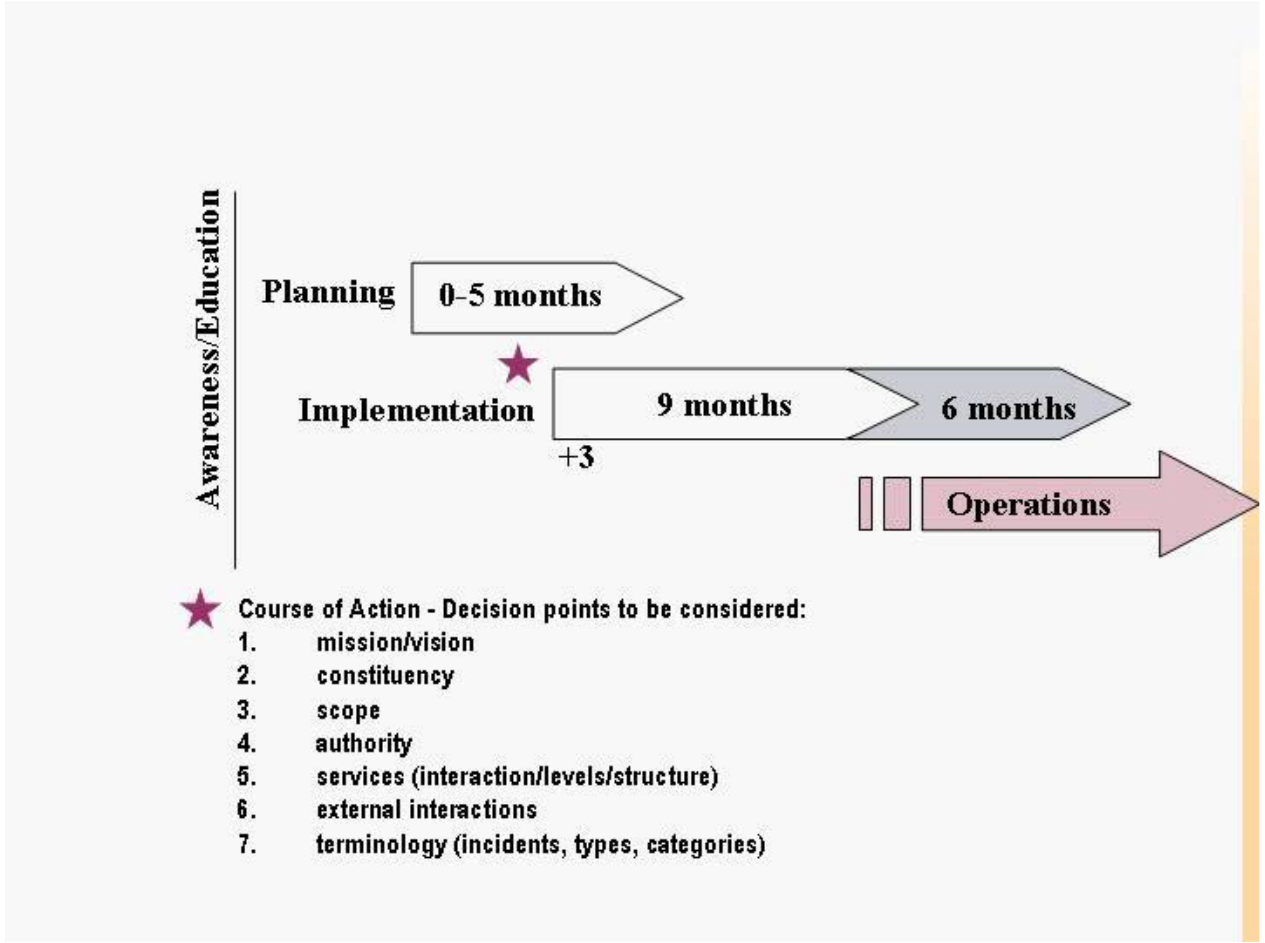
PLANNING

IMPLEMENTING PHASE

OPERATING PHASE

COLLABORATION

Time needed for organization establishment



Type of services

Reactive	Proactive
Incident Response and Handling	Watch and Warn / Threat Monitoring
Security Operation Centre (SOC)	Applied Research
Security Advisory & Alerts	Tools development
Cyber Security Crisis management	Malware Analysis
	Security Advisory & Alerts
	Awareness management

Challenges in creation of security response teams

- Cooperation with various parts
- Staffing and skills with expertise
- Budget
- Quality of provided/expected service
- Change in nature of incidents

Benefits of having security response teams

Serve	serve as a trusted point of contact
Develop	develop an infrastructure for coordinating response to computer security incidents within a scope of activity
Develop	develop a capability to support incident reporting across a broad spectrum of sectors
Conduct	conduct incident, vulnerability, and artifact analysis
Participate in	participate in cyber “watch” functions
Provide	provide language translation services for technical analyses of malicious code and other computer security information from external entities
Make	make general security best practices and guidance available through publications, web sites, and other methods of communication.

Organization structure

Human resources

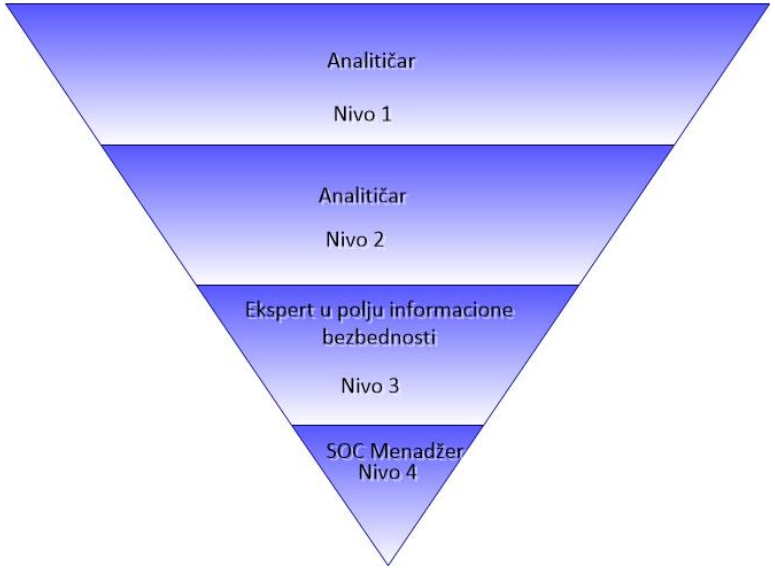
Software tools: SIEM, vulnerability testers, incident management software etc.

Hardware: server and communication devices

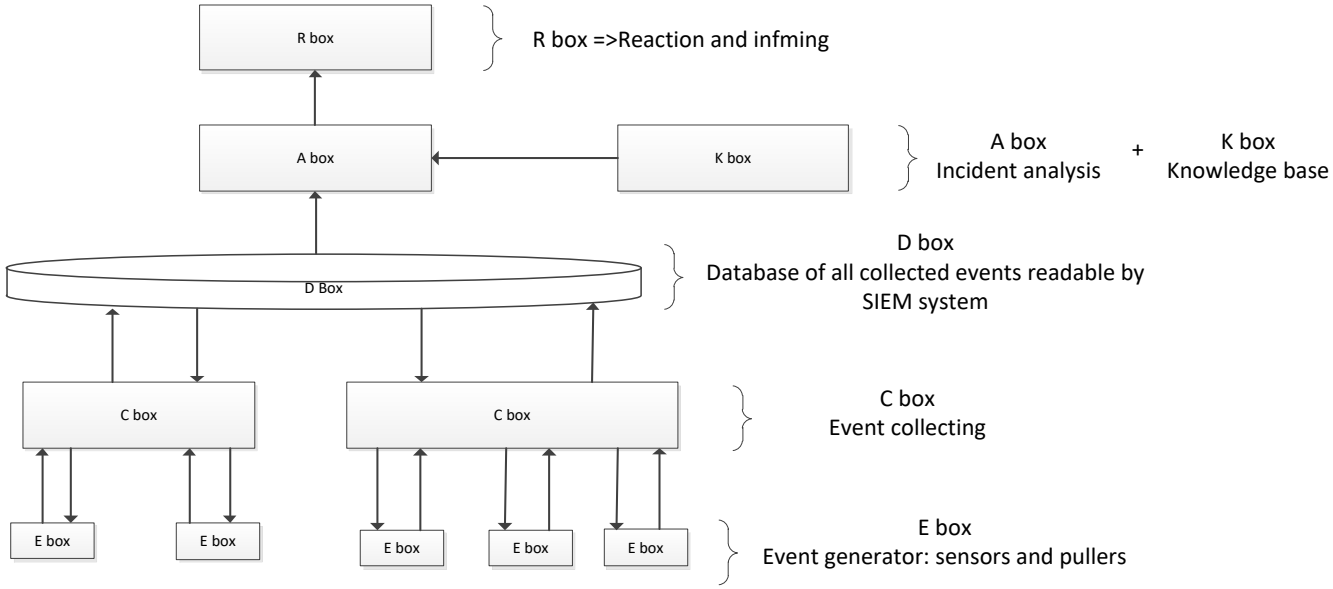
Physical and logical assets and security

Human resources

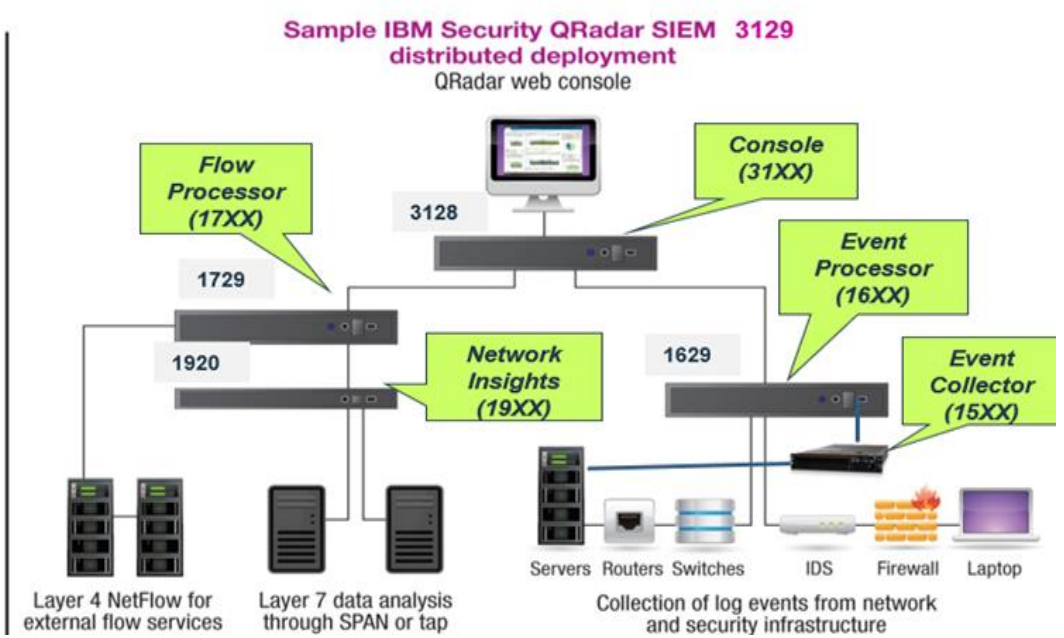
Nivo	Naziv	Opis	Veštine	Odgovornosti
1	Analitičar	Specijalistička trijaža	Veštine sistem administratora (Linux/Unix/Mac/Windows/Databases); poseduje znanja iz oblasti sistemskog programiranja i veština iz oblasti bezbenosti (CISSP, GCIA, etc.)	Proverava poslednje alarme sa ciljem određivanja relevantnosti i hitnosti. Kreira nove servisne tikete za alarme koje je potrebno istražiti na narednom nivou. Pokreće testove ranjivosti i revidira dobijene izveštaje iz istih. Upravlja i konfiguriše alate za kontrolu bezbednosti IT infrastrukture (netflows, IDS, korelaciona pravila itd)
2	Analitičar	Odgovara na incidente	Sve gorenavedene + prirodne sposobnosti, izraženost radoznalost da dođe do korena problema i sposobnost da normalno rade pod pritiskom. Aktivnosti white hat hakera je velika prednost.	Vrši pregled servisnih zahteva (tiketa) kreiranih od strane Analitičara nivoa 1. Koristi threat inteligence alate (IOCs, bezbednosna pravila itd.) sa ciljem identifikacije sistema pogođenih napadom. Vrši pregled i prikuplja podatke i informacije sa sistema (konfiguracije, aktivne procese itd.) zbog potreba buduće istrage. Određuje i upravlja procesom remedijacije i oporavka.
3	Ekspert u polju informacione bezbednosti	Zadužen za detektovanje ranjivosti na sistemima	Sve prethodno navedeno+familijaran sa korišćenjem alata za vizuelizaciju podataka (npr. Maltego) i alata za penetracijsko testiranje (npr. Metasploit)	Vrši pregled kompletnog inventara računarskog sistema i testova ranjivosti sistema. Istražuje potencijalne skrivene ranjivosti sistema koji se mogu iskoristiti u okviru računarske infrastrukture koristeći raspoložive alate. Vrši penetracijska testiranja na produkcionim sistemima kako bi otkrio slabe tačke sistema. Predlaže optimizaciju alata za monitoring i zaštitu na osnovu otkrivenih ranjivosti i slabosti
4	SOC menadžer	Upravljanje operacijama u okviru SOC-a	Sve prethodno navdeno+izražene sposobnosti upravljanja i komunikacije	Vrši nadgledanje aktivnosti kompletnog SOC-a. Traži, zapošljava, obučava i ocenjuje osoblje u okviru SOC-a. Pravi i obavlja aktivnosti upravljanja incidentnim situacijama sa direktorima informacione bezbednosti kao i ostalim zainteresovanim stranama. Vrši kontrolu usklađenosti i učestvuje u procesu revizija. Vrši evaluaciju kompletnog SOC-a i predstavlja planove i aktivnosti menadžmentu



Functional organization of incident management



Incident management collecting architecture



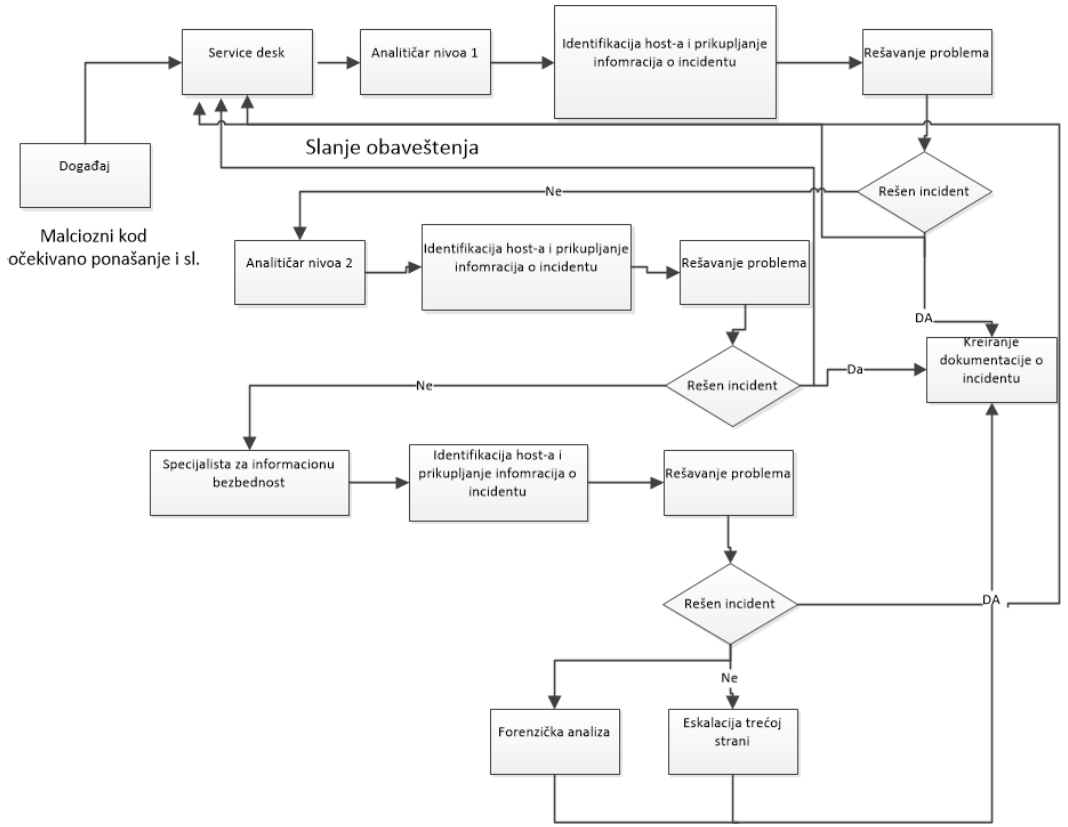
All-in-one represents one device which is used for collecting events and flow records from different sources, performs correlation and evaluating against predefined rule sets as well as creation of alarms related to security incidents

Distributed architecture contains more different devices with different purposes:

- Event/Flow collector
- Event/Flow processor
- Console
- Data nodes

Incident management process

- During the creation of the Incident management process please be aware that it can be very complex and that it can not be completed in one day



Incident reaction and escalation