





# Security Operations Centers

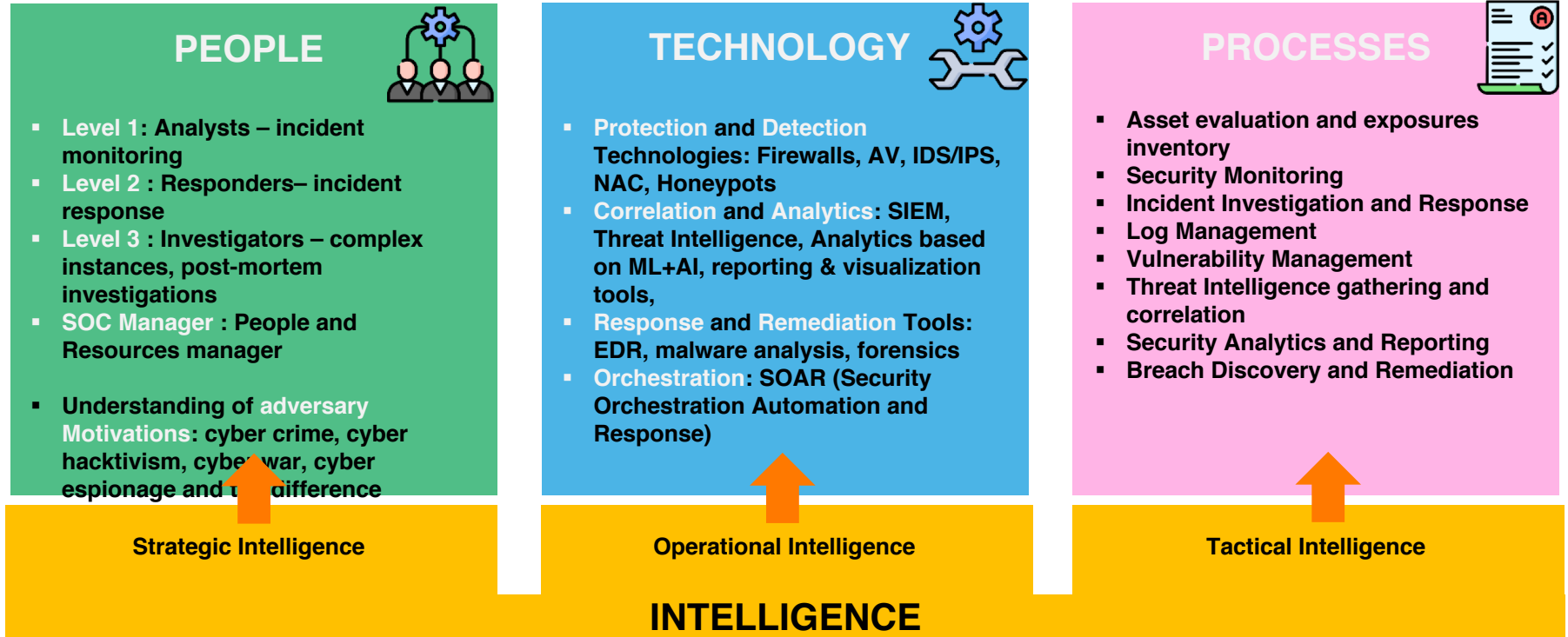
**Ioan Constantin**  
**Orange Romania**



# SOC 1-0-1:

-  A Security Operations Centre (SOC) is a centralized unit that deals with security issues on an organizational and technical level
-  The Cybersecurity SOC (CSOC) consolidates under one organization functions of: incident monitoring, detection, response, coordination and computer network defense tools engineering, operation, and maintenance
-  Computer Emergency Response Team (CERT) are expert groups that handle computer security incidents. Alternative names for such groups include computer emergency readiness team and computer security incident response team (CSIRT). In many organizations the CERT team evolves into an information security operations center (or CSOC).
-  The acronym “CSIRT” is the most technically accurate term that may be used in reference to the team of personnel assembled to find and respond to intrusions. However, its usage is far from universal, most CERTs go by some designation other than “CSIRT,” and its usage has waned in recent years. As a result, identifying them by name alone is not always easy. Many (if not most) cybersecurity professionals use “SOC” colloquially to refer to a CSIRT 😊.

# SOC 1-0-1:



# SOC Process in the Education & Research Context



- Define the assets and the scope
- Define the team and the processes
- Assess exposures, vulnerabilities and weaknesses
- Assess compliance requirements

**ASSETS and SCOPE:** Networks, Devices, End-Points, Testbeds, Physical Security Sensors, Information Publishing and Sharing Platforms, Intellectual Property

- Detection of all cyber and physical threats to assets;
- Analysis of all ongoing threat activity and past threats;
- Artefacts collection for post-incident activities

**THREATS:** Malware, Denial of Service, Data Exfiltration, Ransomware, Data Leakage, Personal Identifiable Information Leakage, Threats to Patents & IP

- 1<sup>st</sup> Line of Defense
- Isolation of compromised assets
- Data Recovery, Information Availability Assurance
- Escalation of complex incidents
- Restoration of compromised assets

- Overview on all threat activity
- Inventory of all assets with compromised availability, confidentiality or integrity of data
- Attribution and contact with authorities
- Knowledgebase of incidents

# SOC Services

## CONTINUOUS SERVICES

### SECURITY MONITORING

- Pre-on-boarding
- On-boarding
- Monitoring

### INCIDENT RESPONSE

- Incident Analysis
- Incident Documentation
- Incident Prioritization
- Incident Notification
- Choosing a Containment Strategy
- Evidence Gathering and Handling
- Identifying the Attacking Hosts
- Eradication and Recovery
- Lessons learned
- Performance monitoring
- Reporting

## ON-DEMAND SERVICES

### VULNERABILITY ASSESSMENT

### PENETRATION TEST

### THREAT HUNTING

### SECURITY MANAGEMENT SERVICES

- Asset Management
- Risk Management
- Education and Training
- Certification

# SOC Continuous Services

**SECURITY MONITORING:** collect and analyze information to detect suspicious behavior or unauthorized system changes in the network, define which types of behavior should trigger alerts, and take action on alerts as needed. Is a reactive service

**PRE-ON-BOARDING:** elaborate and formalize all details (services to be delivered, how to be delivered, SLA, governance, etc.) between SOC supplier and the Client

**ON-BOARDING:** implement all needed steps in order for SOC to deliver the services. It includes the preparation phase (part of incident response process)

**SECURITY MONITORING** is based on monitoring the logs (events) from all assets in supervised perimeter (log aggregation, normalization and correlation – that leads to alerts) and on notifications coming from client personnel

## **SOC** Continuous Services (2)

**INCIDENT RESPONSE:** investigate and resolve the alerts that are confirmed to be security incidents with the aim to minimize loss or theft of information and disruption of services.

**INCIDENT ANALYSIS:** assessment performed on the existing information (precursors, indicators, data, statistics, facts, evidences) to determine: the scope (which networks, systems, or applications are affected); who or what originated the incident; and how the incident is occurring

**INCIDENT DOCUMENTATION:** record all facts associated to the incident

**INCIDENT PRIORITIZATION:** determine the order of treating the incidents based on functional impact, information impact and recoverability from the incident

**INCIDENT NOTIFICATION:** inform and involve all needed parties to play their roles (systems/assets owners, information security)

**CHOOSING A CONTAINMENT STRATEGY:** select the method to effectively cover and eradicate the attack, as well as to successfully recover from it

# SOC Continuous Services (3)

**EVIDENCE GATHERING AND HANDLING:** collect the information in a professional manner with primary goal to resolve the incident; the secondary one is to use for legal proceedings

**IDENTIFYING THE ATTACKING HOSTS:** reveal the identity (IP address) of the attacker

**ERADICATION AND RECOVERY:** define and implement tasks to suppress the incident and regain asset / service's functionality

**LESSONS LEARNED:** post-mortem analysis with the aim to prevent similar incident and improve the response

**PERFORMANCE MONITORING:** monitor all tools that are included in SOC tools ecosystem together with the interaction between SOC tools ecosystem and monitored assets

**REPORTING:** produce and deliver activity reports that include the KPIs agreed in pre-on-boarding phase



# SOC On-Demand Services

**VULNERABILITY ASSESSMENT:** identify, quantify and prioritize system weaknesses in order to apply a patch or fix to prevent a compromise. It is a comprehensive look at the security posture of the organization. The completed assessment includes analysis of both internal and external threats and vulnerabilities

**PENETRATION TEST:** test a computer system or network to find vulnerabilities that an attacker could exploit. Includes internal and external penetration testing

**THREAT HUNTING:** proactively search for cyber threats that are waiting undetected in the network. Cyber threat hunting digs deep to find malicious actors in the organization environment that have overpassed organization's initial endpoint security defenses

## SECURITY MANAGEMENT SERVICES

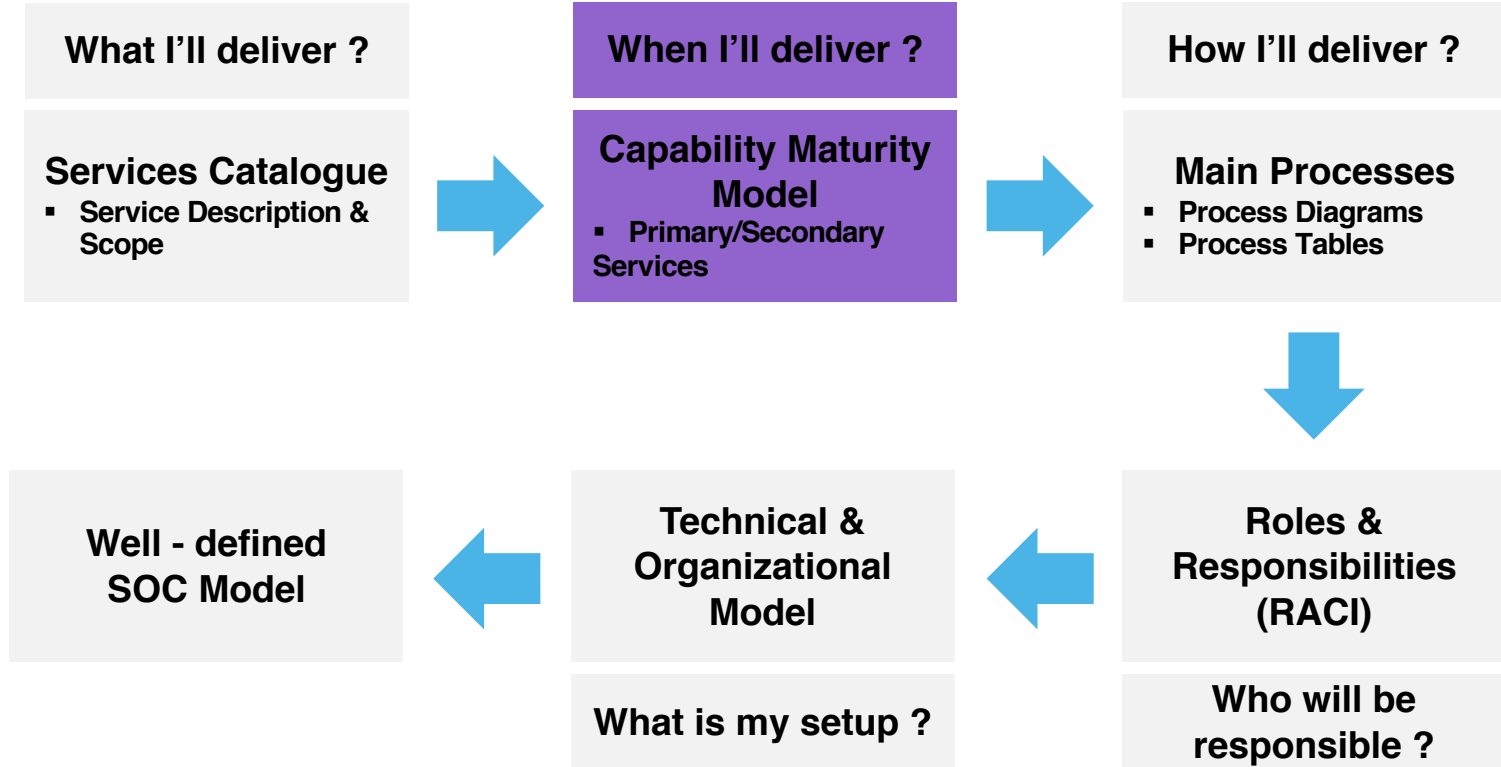
Asset Management

Risk Management

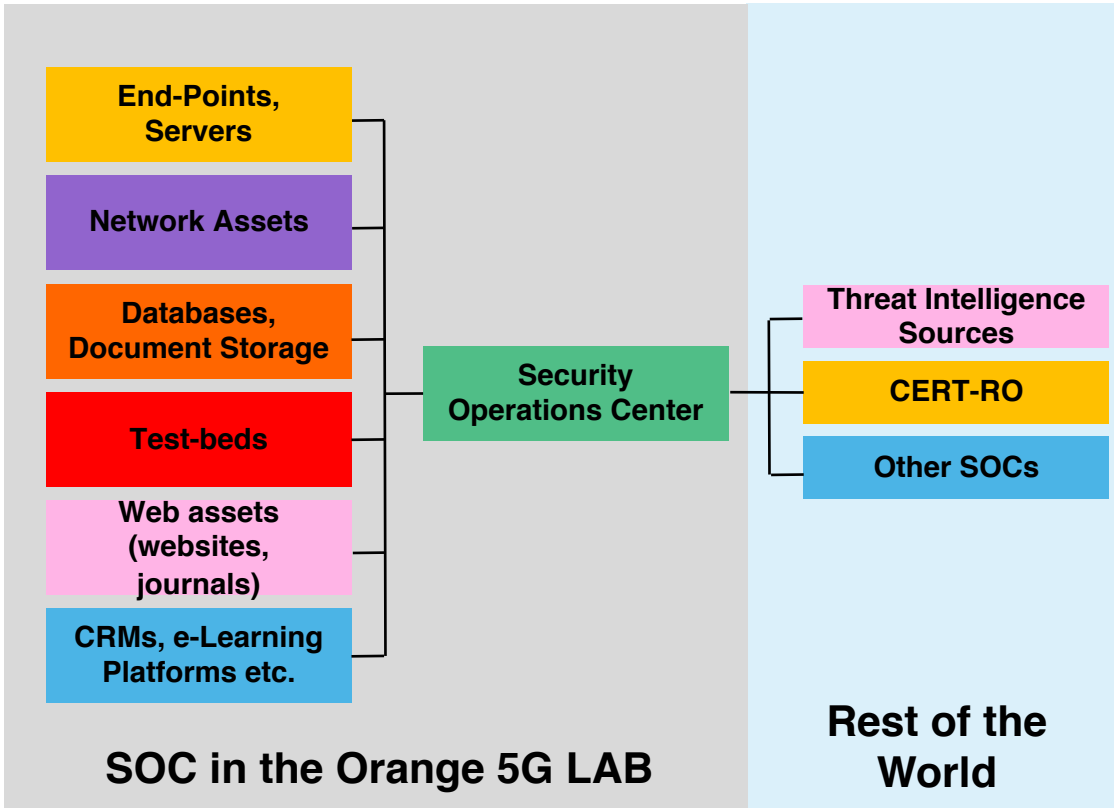
Education and Training

Certification

# SOC Journey



# SOC People & Technical Resources



## SOC - the team



Manager



Level 3

Investigators: 1 - 2 grad/doc/post-doc, extensive cyber security knowledge is required



Level 2

Responders: 2 - 3 grad/undergrads, some cyber security knowledge is required



Level 1

Monitoring: 2 - 3 students, no cyber security background required

# SOC Technology

Hybrid Approach to integration: Mix of open source, commercial and free software		
Technology	Can integrate and reuse existing components?	Proposed components
SIEM	<input checked="" type="checkbox"/>	Elastic SIEM
Endpoint Detection & Response (EDR)	<input checked="" type="checkbox"/>	Elastic Endgame
Anti-Malware	<input checked="" type="checkbox"/>	Elastic Endgame
Sandboxes	<input checked="" type="checkbox"/>	Cuckoo Sandbox
Honeypots	<input checked="" type="checkbox"/>	Cowrie, Honeything, ConPot, ElasticHoney, Thug etc.
IPS/IDS	<input checked="" type="checkbox"/>	SNORT, SecurityOnion etc.
Exposure Assessment	<input checked="" type="checkbox"/>	Orange TEMP, OpenVAS, Sucuri etc.
Data Leakage Prevention	<input checked="" type="checkbox"/>	Elastic Endgame