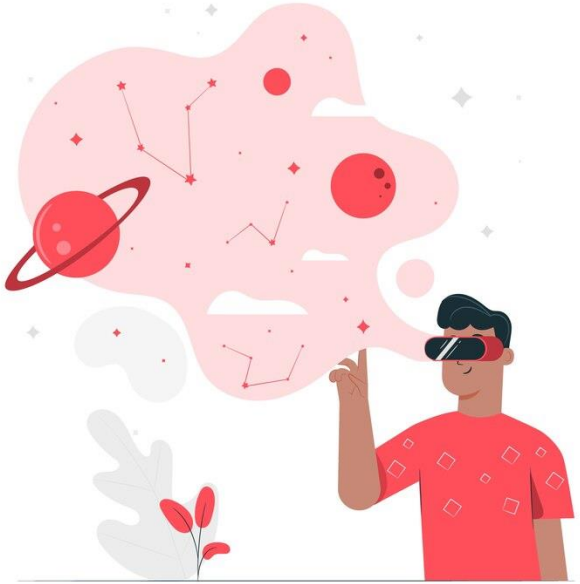
pwc

NEXT
Technology Solutions

The Ins & Outs of the SOC Analyst Role



About Me

- Got to know the cyber security field as an InfoSec Officer @ IDF.
- ~11 years of experience
- SOC-related roles:
    - Served as a SOC Analyst, SOC Manager and DFIR Investigator @ Intelligence Directorate
    - SOC Analyst @ DellEMC MSSP SOC
    - API Security SOC Manager @ Salt Security
- Today: Cyber Security Architect @ PwC NEXT - Assisting organization to build and improve SOC teams
- B.Sc. Computer Science, M.A. Law, CISO, DPO, AWS Security

3 Types of SOC

1 In-house SOC

Its purpose is protecting the organization in which it resides in.

Protection goals:
- Business functions
- Confidential info
- PII

High-level management by CISO.

Includes all tiers.

Working with Security Engineers, Security Architects, GRC, DevSecOps, Application Security – For guidance and cooperations.

IDF

2 MSSP SOC

Its purpose is performing initial triage for client organizations.

Provides 24/7 Tier-1 SOC (sometimes Tier-2 as well).

Directed mainly by Customer Success approach.

Example:
- QMasters
- Trustnet

DellEMC

3 MDR (Managed Detection and Response)

Its purpose is protecting client organizations on a specific subject or solution, and for improving the solutions developed by the company.

Using of not standard SOC tools.

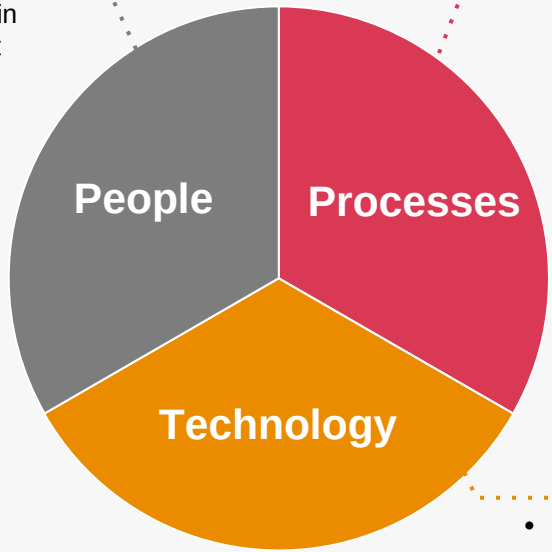
Examples:
- SentinelOne – EDR
- Radware – WAF & DDoS
- Salt – API Security

Working with Product, R&D, Customer Success (TAM), Sales Engineers.

Salt

SOC Components

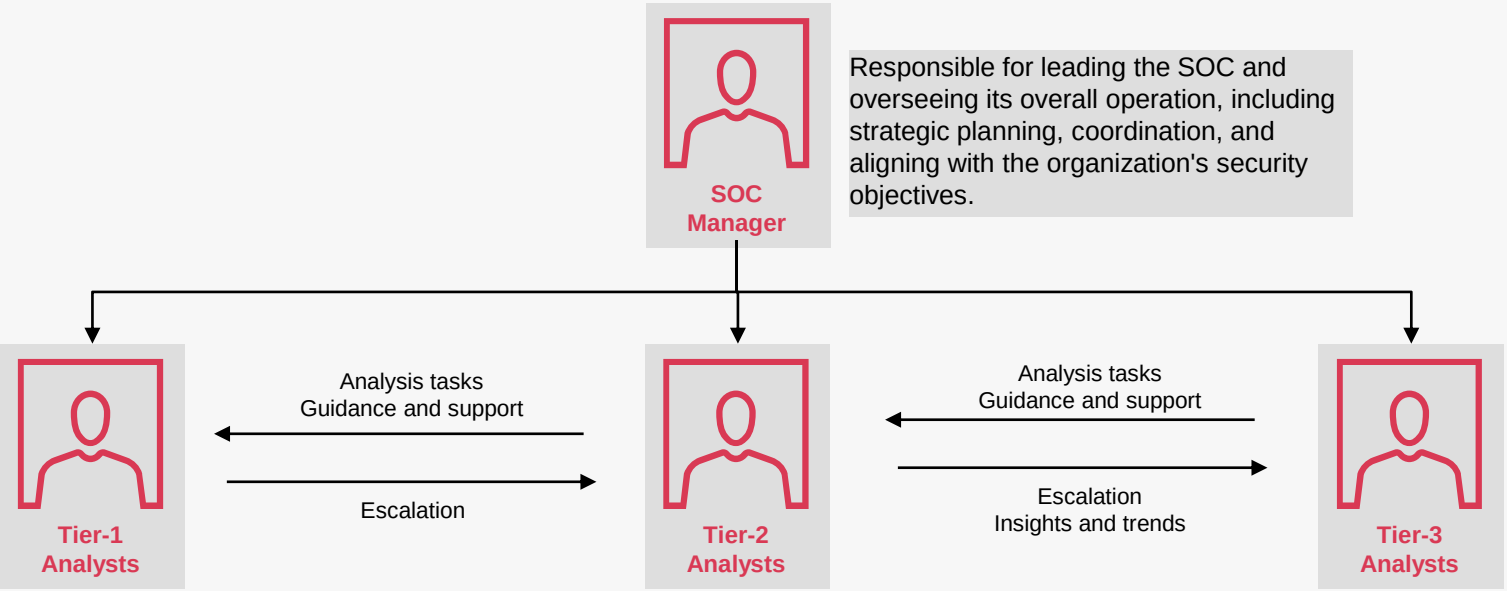
- Hiring – Getting and right person for the role in the matter of knowledge, experience and soft skills.
- Structure – Build your SOC to support your objectives. Update it all the time.
- Training – Have a training plan for a new analyst. On-going training for existing analysts.



- Procedures:
  - Detection and identification
  - Investigation
  - Mitigation
  - Escalation
  - Communication

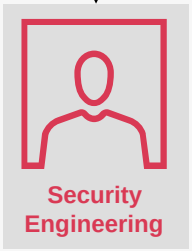
- SIEM – Log sources, rules
- EDR
- SOAR and proper playbooks
- Access to log sources – AV, FW, IDS, MDM, VM, etc.

SOC Structure



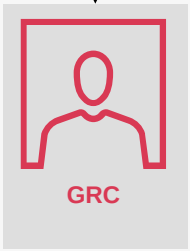
In-house SOC Position

CISO is a senior-level executive who oversees an organization's information, cyber, and technology security. The CISO's responsibilities include developing, implementing, and enforcing security policies to protect critical data and the continuity of business functions.



Implement, integrate, configure, operate and troubleshoot security solutions according organization's security objectives

Design and provide assisting in designing secure architectures and processes



Development and enforce policies and procedures, prepare for cyber regulation compliance, assess cyber risks.

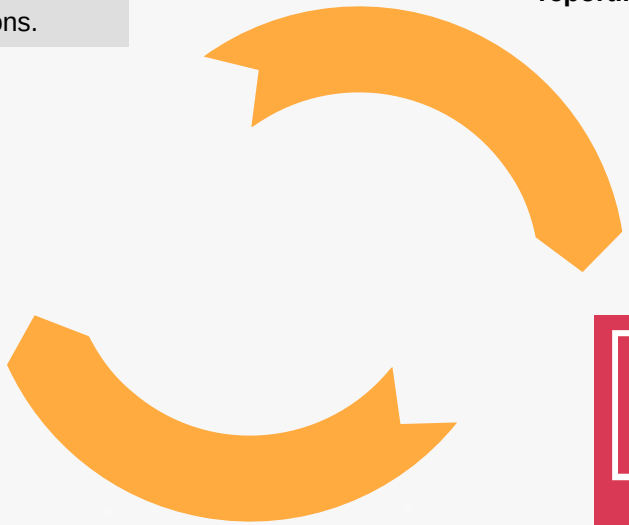
Responsible for the security of the solution the organization develops:
CI/CD
Secure coding

Responsible for leading the SOC and overseeing its overall operation, including strategic planning, coordination, and aligning with the organization's security objectives.

In-house SOC Relationships

CISO is a senior-level executive who oversees an organization's information, cyber, and technology security. The CISO's responsibilities include developing, implementing, and enforcing security policies to protect critical data and the continuity of business functions.

Set events and scenarios which affect confidential data security and critical business functions, SLAs, reporting and communication requirements.



Report regarding security insights and trends effecting data security and business continuity, or might do so in the future.

In-house SOC Relationships

Implement, integrate, configure, operate and troubleshoot security solutions according organization's security objectives

Security Engineering

Providing instructions and guidance for new security solutions.

Set troubleshooting procedures.

Report issues for troubleshooting.

Recommend configuration changes for better detection (more TP, less FP).

SOC

In-house SOC Relationships

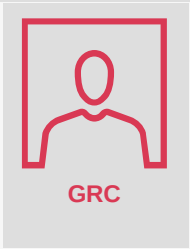
Design and provide assisting in designing secure architectures and processes

Providing info regarding new security control implemented or changes in existing ones, that SOC might need to monitor.

Develop monitoring queries, widgets and dashboard for security controls and achieving those goals.

In-house SOC Relationships

Development and enforce policies and procedures, prepare for cyber regulation compliance, assess cyber risks.



Checking whether risks (likelihood X impact) can be reduced using proper detection, identification and mitigation procedures. Verifying all incidents are responded properly.

Providing Key Risk Indicators (KRIs)

In-house SOC Relationships

Design and provide assisting in designing secure architectures and processes

DevSecOps

Providing application security training, knowledge and tools.

SOC

Develop monitoring queries, widgets and dashboard for application security and report on findings.

MSSP SOC Position

Customer

The customer entity consists of:

- CISO
- Tier-2 and Tier-3 SOC analysts

Customer Success Manager

- On-boarding process
- Checking with the customer and make sure for: Business and technical satisfaction, needs fulfillment and proper SLA.
- Liaison between customer and SOC
- Support
- Optimizing renewal and avoiding churn

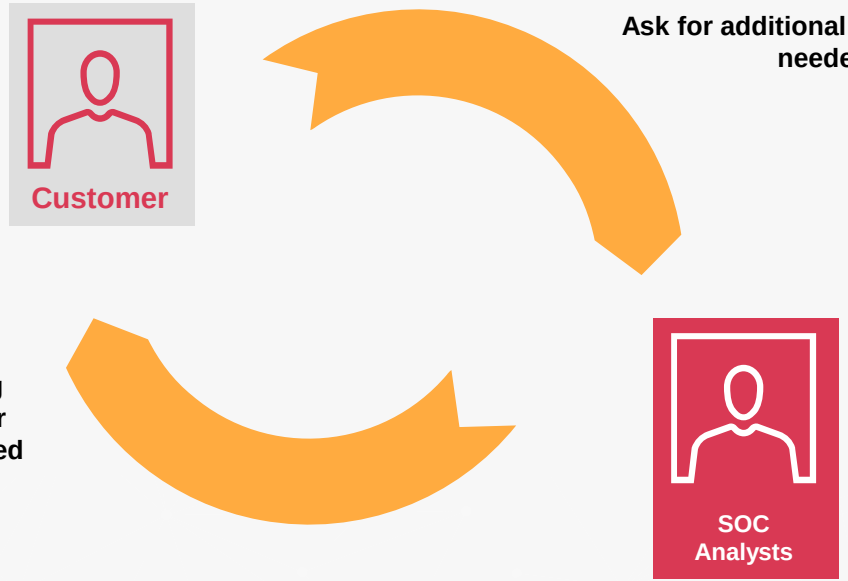
SOC Manager

Responsible for leading the SOC and overseeing its overall operation, including strategic planning, coordination, and aligning with the customer's security objectives and needs.

SIEM Integrator

Connecting logs source to SIEM, parses and normalizes logs.

MSSP SOC Relationships



Ask questions about Tier-1 report for clarification.

Ask for additional analysis when needed.

Provide Tier-1 triage reports, including trigger, findings, recommended further analysis and investigation, recommended mitigation, and suggesting prevention methods.

MSSP SOC Relationships

Present customer's security objectives and needs.

Check for deviations for the above.

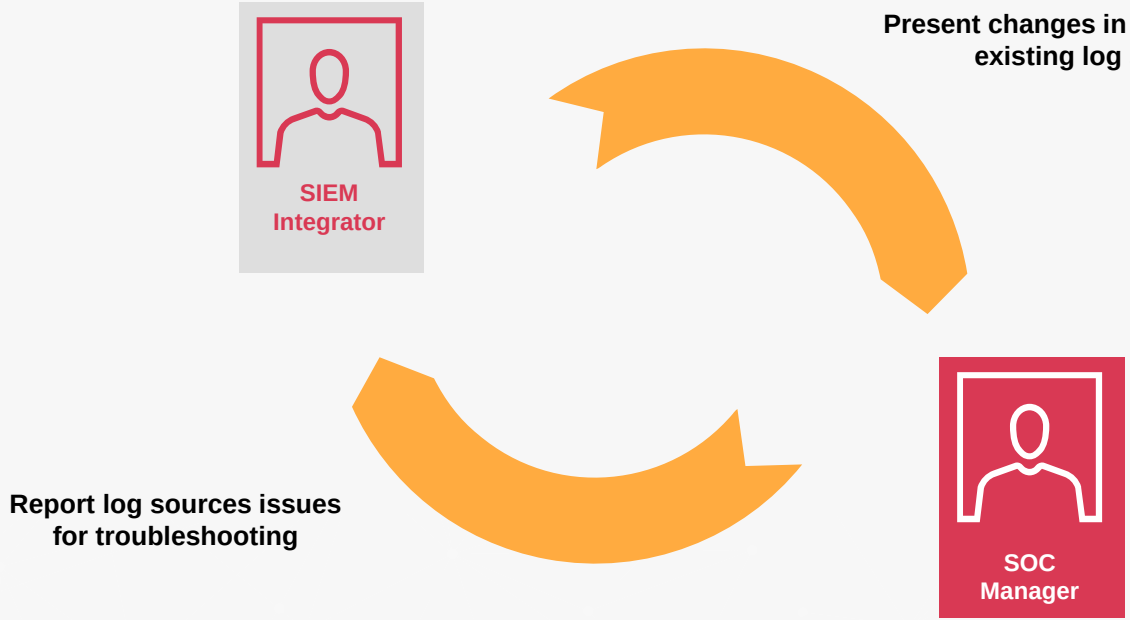
Present technical issues for troubleshooting.

Present tailor-made solutions for customer's objectives and needs.

Report issues threatening customer's satisfaction.

Report regarding security insights and trends for providing customer value.

MSSP SOC Relationships



Essential Backgorund: Solution Sales Process to a Customer

Get Sales Leads

By: Business Development

They research for:

- What business sectors and what geographical areas needs our solutions?
- What companies are within those sectors and fields?
- Who is the relevant stakeholder in each company?

Sales Engineering

By: Sales Engineer

Sales process:

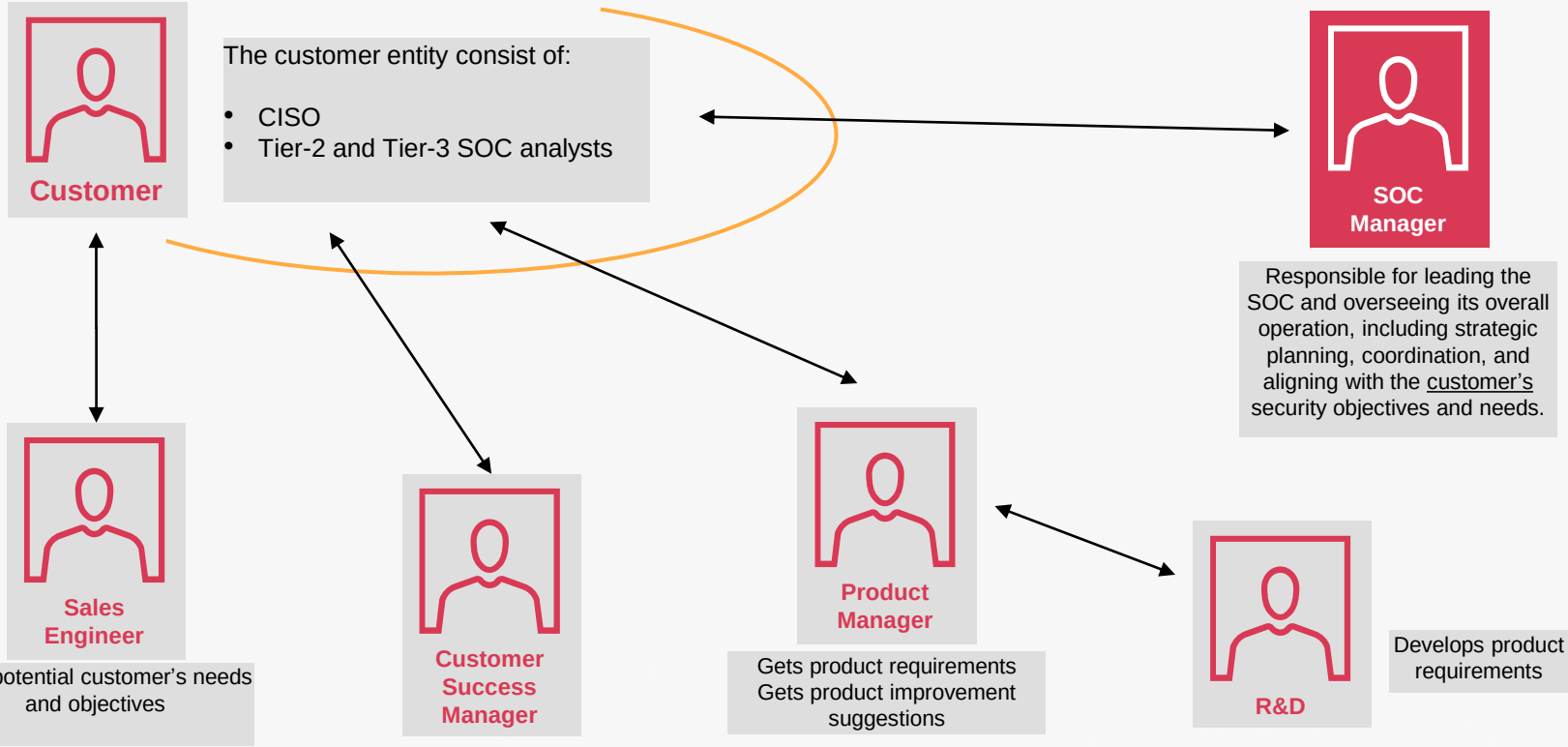
- Reach out to relevant stakeholder, set a meeting, present solution
- Understand his objectives and needs
- Conduct a PoC/PoV
- Sign a contract
- Update Customer Success Department

Customer Success

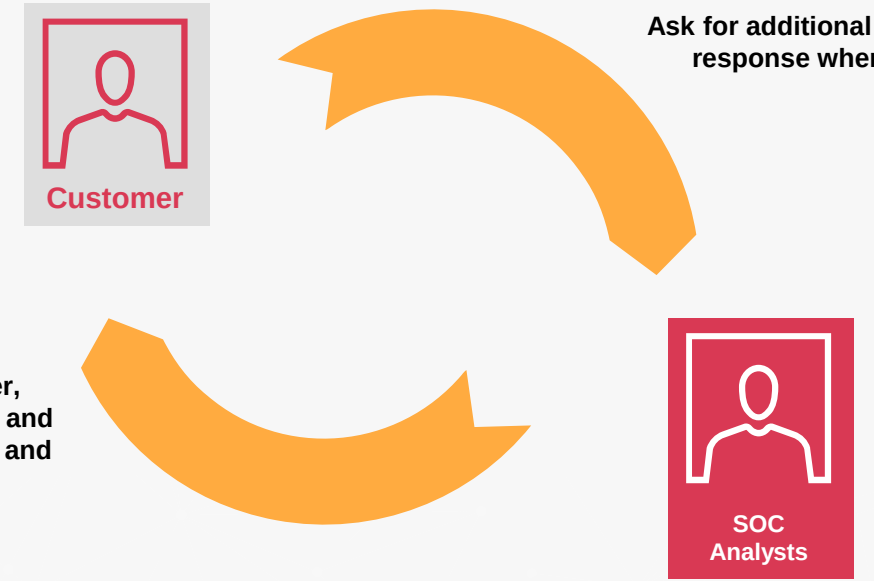
By: Customer Success Manager

- On-boarding
- Monitor customer objectives and needs fulfillments
- Technical support
- Renewal

MDR SOC Position



MDR SOC Relationships

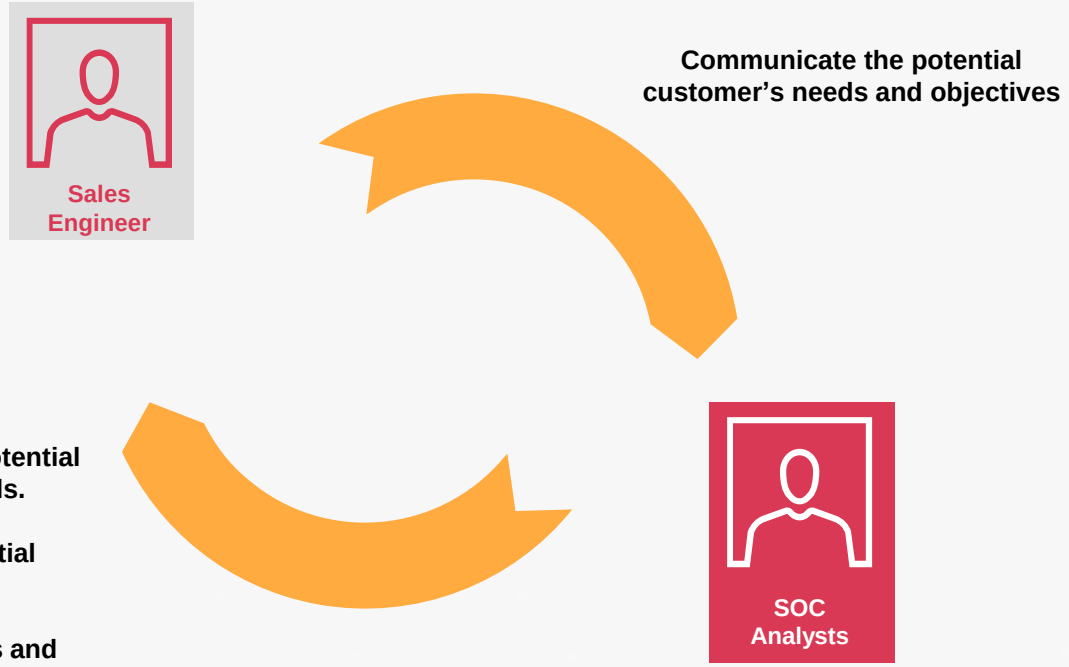


Ask questions about report components for clarification.

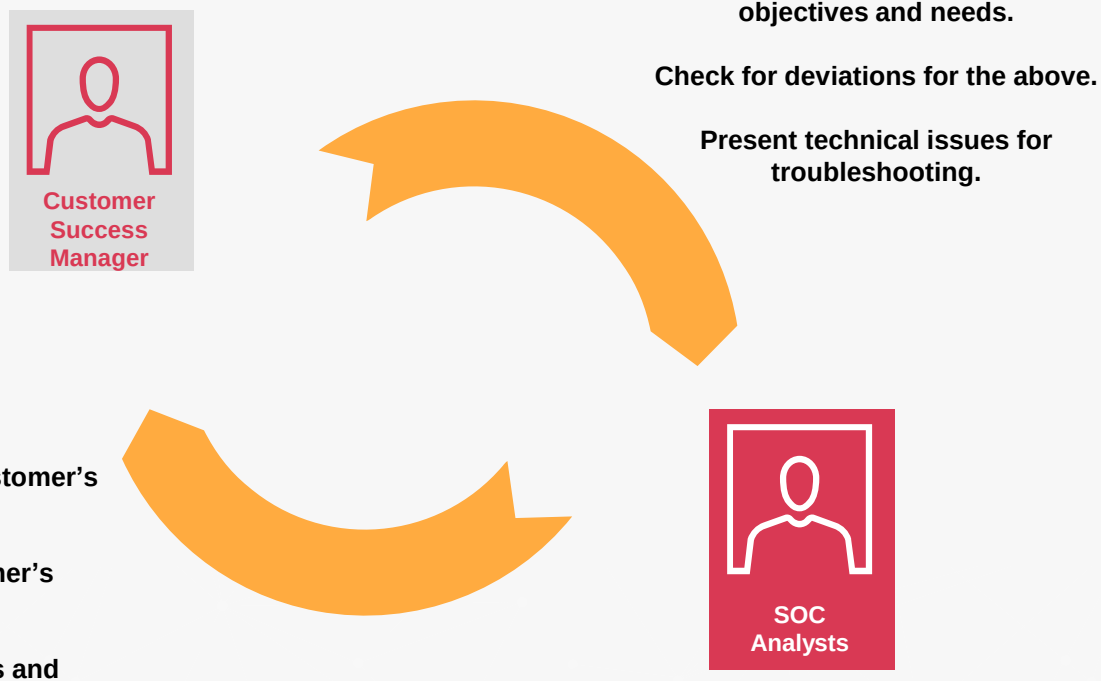
Ask for additional analysis and response when needed.

Provide triage report, including trigger, findings, recommended further analysis and investigation, recommended mitigation, and suggesting prevention methods.

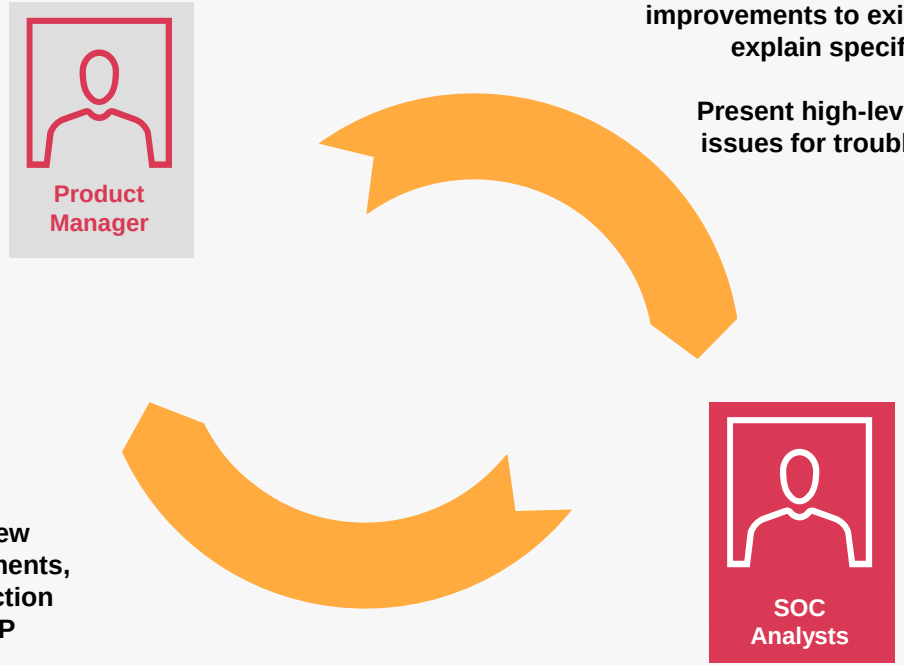
MDR SOC Relationships



MDR SOC Relationships



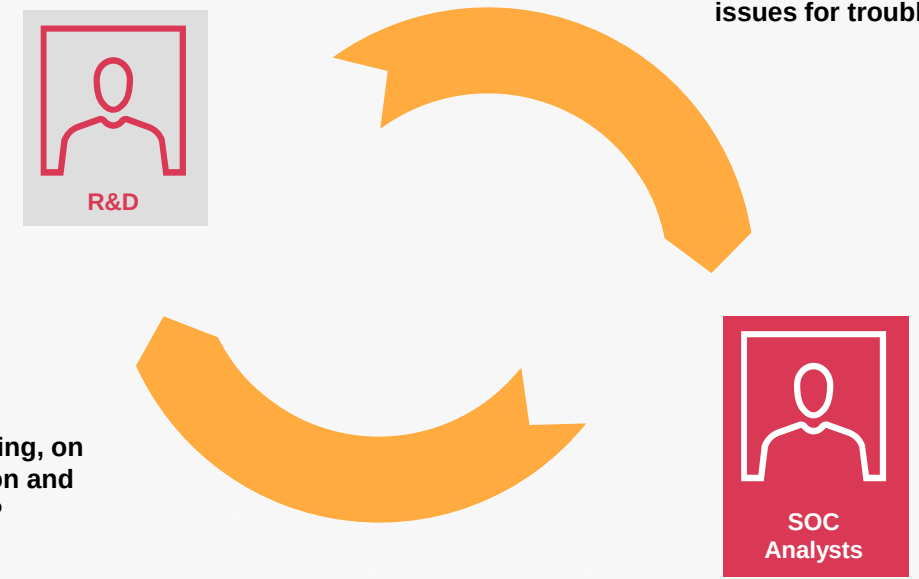
MDR SOC Relationships



MDR SOC Relationships

Present fixed bugs.

Present low-level technical issues for troubleshooting.



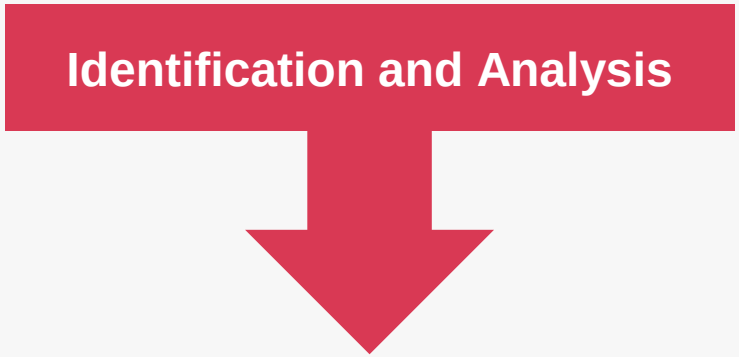
Provide suggestions bug fixing, on emphasis on better detection and response, and less FP

SOC Work Scheme

	24/7 Shifts	“Follow the Sun”
	Morning, evening and nights. Analysts from the organization’s main region.	Day shifts only Analysts from at least 2 of the organization’s main regions.
Advantages	Easier to manage and communicate.	Analysts are “fresh” to tackle new incident anytime.
Disadvantages	Burnout – Analysts tend to leave the organization after a while for day-only job. Need to hire and training new ones.	Cultural differences Less supervision

Common Response Workflow

Network alert
Security alert
Anomaly
Interruption / Outage



How can we block the attack and return to normal state?

What is happening?
What attack is taking place?

(מה, מי, מקום, מועד, מדוע ואיך)

Report Scheme

Initial Trigger

What log source triggered it?
What was the incident about?
What can you understand from it?
What are the potential root causes?
Where can it be false positive?

Investigation

Investigations methods

Findings and their meaning

Actions you took

Conclusions

Root cause assumption / False positive

Additional explanations

Recommendations

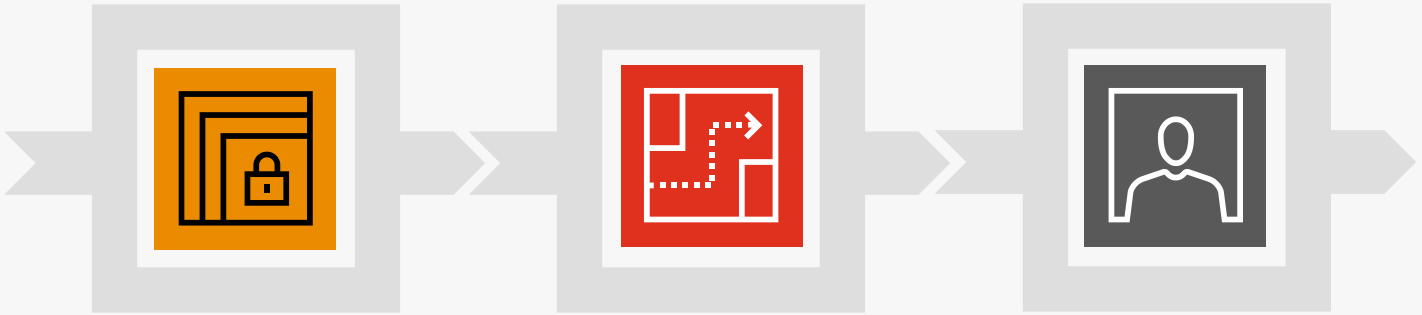
Additional investigation needed

How can the client mitigate the attack?

How can we prevent similar attacks in the future?

Reactive vs. Proactive

From Technology to Processes to People



Technology

Create rules that can detect a security incident, not only during and after it happens, but even before.

Processes

Not only responding to SIEM alerts, but conducting on-going threat hunting activities.

People

People should identify gaps in our SOC. And when they do, don't just ignore them or complain about them – Create solutions.

The (Endless) Learning Process

Academic Studies

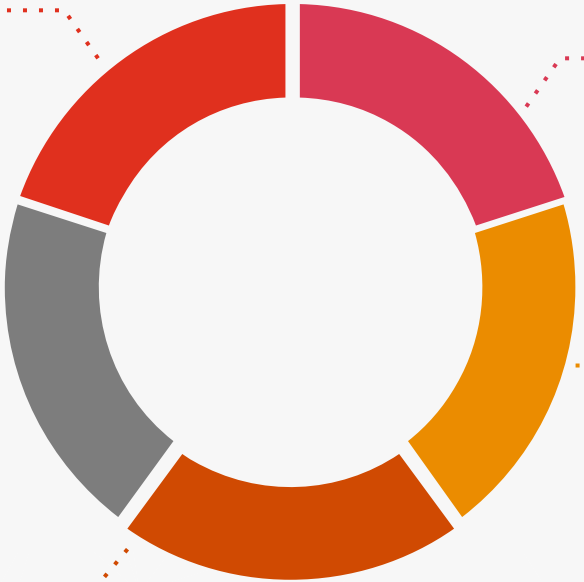
B.Sc. / B.A. – Technical
M.A / MBA – Management

Professional Studies

Network Vendors
Cloud Vendors
CISO

Subject-level and Vendor Studies

Networking, API Security, CVSS, CTI,
MITRE ATT&CK, Malware Analysis, GRC…



Hands-on Training

API Security, AV, CSPM, DLP, EDR,
IDS, MDM, NAC, Sandbox, SSPM, WAF, etc.

Scripting
(mostly Python and PowerShell for automation)

Personal Contribution

Projects
Articles
LinkedIn posts

Hiring Process

NEXT
Technology Solutions

Talent Acquisition Partner

Checks basic fit to requirements

Validates CV

Hiring Manager

Technical questions

Technical on-site/home assignment

Checks fit to role duties and team's vibes by hard and soft skills

Hiring Manager's Manager

Technical questions

Checks fit to company's objectives

Seeing the bigger pictures

HR

Responsibility
Motivation
Conflict resolution
Handle difficulties
Assisting other people

Contract Signing

Set your goals

Set what important to you and what isn't

What Does Hiring Manager look for?

Hard Skills

- Network
- Cyber security concepts
- Security solutions
- Cloud security
- Role-specific knowledge

Soft Skills

- Eager to learn and work
- Fast learning
- Someone we can relay on
- Verbal communication
- Written communication
- Being proactive

Training Process

- Network
- Cyber security
- Cloud security
- Role-specific knowledge

- Knowledge base
- Team procedures
- Security solution stack
- Tools

You basically sit beside someone who works…

Now you work and he supervises you

You are a SOC analyst !

Interview Q&A

Hard Skills

- Network
- Cyber security concepts
- Security solutions
- Cloud security
- Role-specific knowledge

Soft Skills

- Fast learning
- Verbal communication
- Written communication

What you answer?

How you answer?

pwc

Interview Q&A

NEXT
Technology Solutions

Question: What is a **three-way handshake** ?

Interview Q&A

Question: What is a **three-way handshake** ?

Answer: A **three-way handshake** is a method used in TCP to create a connection between a client and a server. It's a **3-step method**:

1) Client sends a SYN packet
2) Server replies with a SYN-ACK packet
3) Client replies with a ACK packet

Interview Q&A

Question: What is **Cryptography** ?

Interview Q&A

Question: What is **Cryptography** ?

Answer: Cryptography is the practice of study of techniques and methods for securing information and communication to protect data from being exposed to a 3rd-party.

Interview Q&A

Question: What is the difference between **Symmetric** and **Asymmetric** encryption?

Interview Q&A

Question: What is the difference between **Symmetric** and **Asymmetric** encryption?

Answer: Symmetric encryption – **Same key** for encryption and decryption;
Faster, but **less secure**.
Asymmetric encryption – **One key** for encryption, **other key** for decryption.
More secure, but required **higher computation resources**.

Interview Q&A

Question: Please mention an encryption algorithm for **data-at-rest encryption**.
Please mention a protocol for **data-in-transit encryption**.
Which one is symmetric and which one is asymmetric ?

Interview Q&A

Question: Please mention an encryption algorithm for **data-at-rest encryption**.
Please mention a protocol for **data-in-transit encryption**.
Which one is symmetric and which one is asymmetric ?

Answer: AES - Symmetric
TLS - Asymmetric

Interview Q&A

Question: What is the **CIA Triad** ?

Interview Q&A

Question: What is the **CIA Triad** ?

Answer: CIA stands for **Confidentiality**, **Integrity** and **Availability**.
It's a model designed to guide policies and processes for Information Security, and one of the most popular one.

Interview Q&A

Question: What is a **data leakage**?
Please mention three types of it.

Interview Q&A

Question: What is a **data leakage**?
Please mention three types of it.

Answer: Data leakage is an event where sensitive data is transmitted from within the organization to an external unauthorized entity.
Three types of data leakage:

1) **Accidental** breach – An employee sends it unintentionally due to a fault or an error.
2) **Intentional** breach – An employee sends it on purpose due to a motive.
3) **Data exfiltration** – Data is stolen by a malware and sent to a hacker.

Interview Q&A

Question: What is a **brute force attack**?
How can you prevent it?

Interview Q&A

Question: What is a **brute force attack**?
How can you prevent it?

Answer: A brute force attack is a **hacking method** that uses **trial and error approach** to **crack passwords, login credentials, and encryption keys**. It is a simple yet reliable tactic for **gaining unauthorized access** to individual accounts and organizations' systems and networks.
The hacker tries **many usernames and passwords combinations** until he find the correct login information.

It can be prevented by:

1) Password minimum length
2) Password complexity
3) Login rate-limiting

Interview Q&A

Question: What is a **DDoS attack**?
How is a different from **DoS**?

Interview Q&A

Question: What is a **DDoS attack**?
How is a different from **DoS**?

Answer: DDoS Attack means **Distributed Denial-of-Service Attack** and it is a cybercrime in which the attacker **floods a server with internet traffic** to **prevent it from providing online services and sites**.

It utilizes thousands (even millions) of connected devices, called a **botnet**, to achieve this goal. This is while in DoS only one device is used.

pwc

Interview Q&A

NEXT
Technology Solutions

Question: What is **XSS**?
How can you prevent it?

pwc

Interview Q&A

NEXT
Technology Solutions

Question: What is **XSS**?
How can you prevent it?

Answer: **Cross-site scripting** (XSS) is an attack in which an attacker **injects malicious scripts** into the code of a trusted website or API **to be executed by legitimate users**.
It can be prevented by **validating and sanitizing user input**.

Interview Q&A

Question: What is a **Multi-Factor Authentication** ?

Interview Q&A

Question: What is a **Multi-Factor Authentication** ?

Answer: Multi-factor authentication (MFA) is a **multi-step account login process** that requires users to enter **more than just a password**.
For example, along with the password, users might be asked to enter a code sent to by SMS, answer a secret question, or scan a fingerprint.

Interview Q&A

Question: What is a **Firewall** ?

Interview Q&A

Question: What is a **Firewall** ?

Answer: **Firewall** is a network security system. It sets the **boundary** of a network.
It **monitors** the traffic **into the network** and **out of it**, and **controls it by rules**.

Interview Q&A

Question: What is the difference between **IDS** and **IPS** ?

Interview Q&A

Question: What is the difference between **IDS** and **IPS** ?

Answer: IDS stands for **Intrusion Detection System**. It uses for **detection only** of a potential attack. It is sometimes placed **out-of-band**.
IPS stands for **Intrusion Prevention System**. It also **takes an action to respond** to a potential attack. It must be placed **in-line**.

Interview Q&A

Question: What is the difference between **HIDS** and **NIDS** ?

Interview Q&A

Question: What is the difference between **HIDS** and **NIDS** ?

Answer: HIDS is **Host IDS**. It is installed on a **server or endpoint** to detect **suspicious behavior**.
NIDS is **Network IDS** to detect **attack traffic patterns**.

Interview Q&A

Question: What is **EC2** ?

Interview Q&A

Question: What is **EC2** ?

Answer: EC2 stands for **Elastic Compute Cloud**.
EC2 is an **on-demand computing service on the AWS** cloud platform.
It also allows the user to configure their instances as per their requirements,
i.e. **allocate the CPU, RAM, and storage needed for the current task.**

Interview Q&A

Question: What is the **Shared Responsibility Model**?

Interview Q&A

Question: What is the **Shared Responsibility Model**?

Answer: The Shared Responsibility Model is a **security and compliance framework** that **outlines the responsibilities of cloud service providers (CSPs) and customers** for securing every aspect of the cloud environment, including hardware, infrastructure, endpoints, data, configurations, settings, operating system (OS), network controls and access rights.

CSP responsible for **“Security of the Cloud”** - Protecting the infrastructure that runs all of the services offered in the cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run cloud services.

Customer responsible for **“Security in the Cloud**” – Access rights, OS patching, network controls, security controls, etc.

Thank You!

For questions
anytime anywhere:

Eran - 0502231881

pwc