**ChapTer 1 : Tools for managing and handling seCuriTy inCidenTs in The enTerprise**

we'll first look at a company's internal structure, how security teams are divided up and how they work together.

1. The different company security teams:

CERT and SOC :

The CERT (Computer Emergency Response Team):

The CERT team is composed of a highly qualified IT security experts in various fields

They are also responsible for reverseengineering ( تفكك حاجة باه تفهم كل عنصر كيفاه يمشي و هاذ الشيئ يخليك تفهم كفاه العناصر مجتمعة مع بعض يخدمو

مثال ..تفكيك كود لفهم كيف يعمل )

of malicious codes to identify and correct security breaches or weaknesses in the company they work for, and develop appropriate solutions to eradicate the risk

CERTs are constantly up-to-date in terms of new attacks, new malware, the latest vulnerabilities and the technologies affected by these vulnerabilities.

The CERT can be an internal team within the company or external (remotely)

The SOC (Security Operations Center):

The SOC can be considered as a control tower . Its responsibility is generally shared between three teams: the security analysts, the SIEM team and the ticketing tools team.

1. The SIEM (Security Information and Event Management) team:

Have 2 teams : RUN and BUILD teams.

The Build Team : design + installation + configuration of SIEM .

* In tne Initial phaseo f SIEM .
* Design . system architecture software integration, and configuration . set up a technology infrastructure that meets the company's needs.
* system deployment or upgrade projects.

The Run Team : maintenance of SIEM ( logs management )

* After system deployment .
* monitoring, incident management, maintenance, and system optimization. They should be able to quickly respond to security events, troubleshoot issues, and keep the system running smoothly.
* monitoring and managing the system on a day-to-day basis.

In summary, the BUILD team focuses on the design and initial implementation of the system, while the RUN team is responsible for the operational management, monitoring, maintenance, and optimization of the system after it is deployed.

1. The Cybersecurity analyst team:

Protect systems, networks and data .

They are responsible for detecting anomalies, breaches and defining appropriate responses to alerts.

Analysts utilize the SIEM tools to collect, correlate and analyze security events logs from various sources .

Analyst 3 levels :

Lvl1 :

- counter phishing emails

- الاستجابة للحوادث : الهدف من الاستجابة للحوادث هو منع الهجمات الإلكترونية قبل حدوثها، وتقليل التكلفة وتعطيل الأعمال الناتج عن أي هجمات إلكترونية تحدث.

- websites exposed to interent without encryption .

Lvl 2 : server prblms

Lvl 3 : define new USecases / fine tuning .

1. The ticketing systems team: is not responsible for the security of the tool, but responsible for the ticketing tool to enable the incidents to be correctly managed and traced.

SOC + CERT work together

Soc = it control tower

Cert = deal with threats

II. Tools for managing and handling security incidents :

Pki / vpn / proxy , reverse proxy / ids , ips / Sandbox .

Some definitions :

Logs : logs are records of all actions taken in a computer system (application, server, router, FW, AV, IPS/IDS, proxy, OS, etc.), including events (e.g. login, connections to an external site, file deletion, USB key connection, etc.) to understand system behavior, track user actions

And all this is is on a file named : LOG FILES …. The log can be transferred in the SIEM tool .

log collection:

It facilitates the work of cyber security analysts by centralizing all logs in a single tool (SIEM).

Anatomy of the log:

a log contains:

- time + action was carried out on a computer system (known as a "timestamp")

- event description

- infos about the user or the machine (username/IP address)

- the action taken by the system/user in question.

Log file could have other infos

The proxy, for example, can provide other logs such as: the website visited, the website domain, the website category, the UserAgent, the destination IP, the destination port, the action taken by the proxy in question, etc .

