
Welcome!!
FDP – Cyber Security (SIEM)
Security Information and Event Mgt.

#whoami

Mahesh Pavaskar (SIEM Architect | Cyber Security & Threat Intelligence Engineer)

Learning never Ends….

12,8+ years of Experience

Education : M. Tech VJTI Mumbai

Research + Industry Background

QRadar 7+ years of Experience
Tech talk no - 64

29+ Certification Cisco Authorized Trainer

BE: Best outgoing Student
Mtech:Student of the Year

Continue……

Source of knowledge base for FDP & Future

- Youtube channel – Free & will be always free
https://www.youtube.com/channel/UCmfJWojrb4UvXqkifBGLu2w

- LinkedIn Profile: https://www.linkedin.com/in/mahesh-pavaskar-88068263/

- Github

❑ Global link

✓ https://github.com/maheshp1987

❑ SIEM link (Specific to topic)

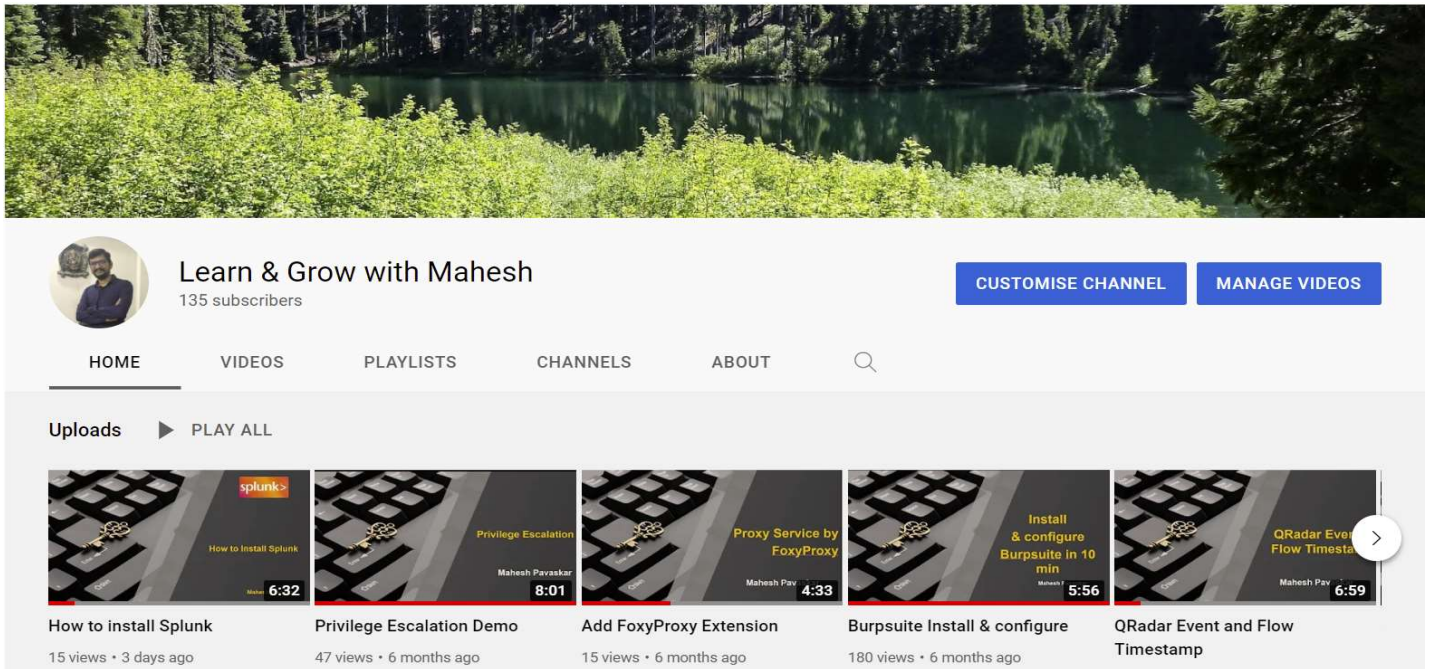
✓ https://github.com/maheshp1987/SIEM

Support & Learn with Me

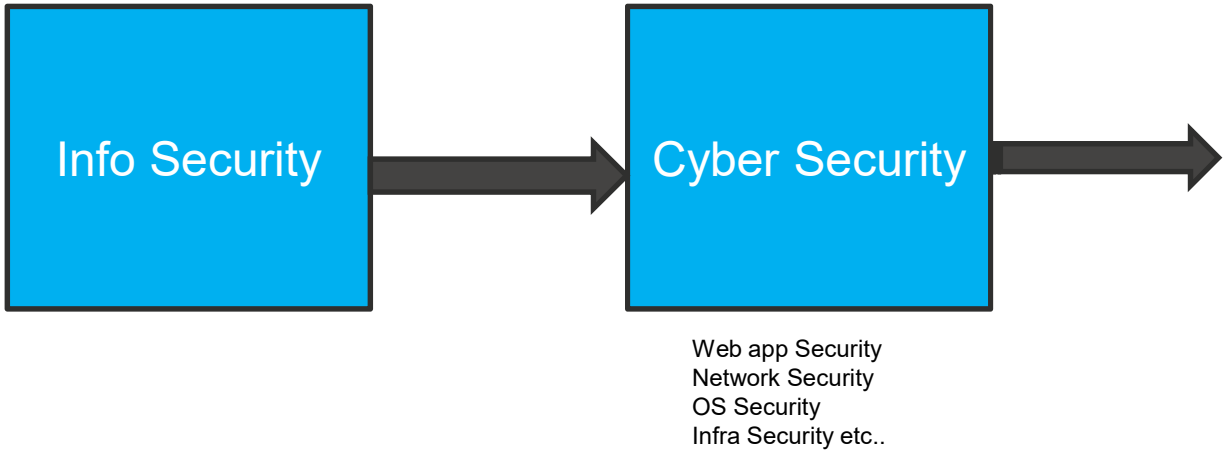
- Youtube channel – Free & will be always free

https://www.youtube.com/channel/UCmfJWojrb4UvXqkifBGLu2w

Channel Name:
Learn & Grow with Mahesh

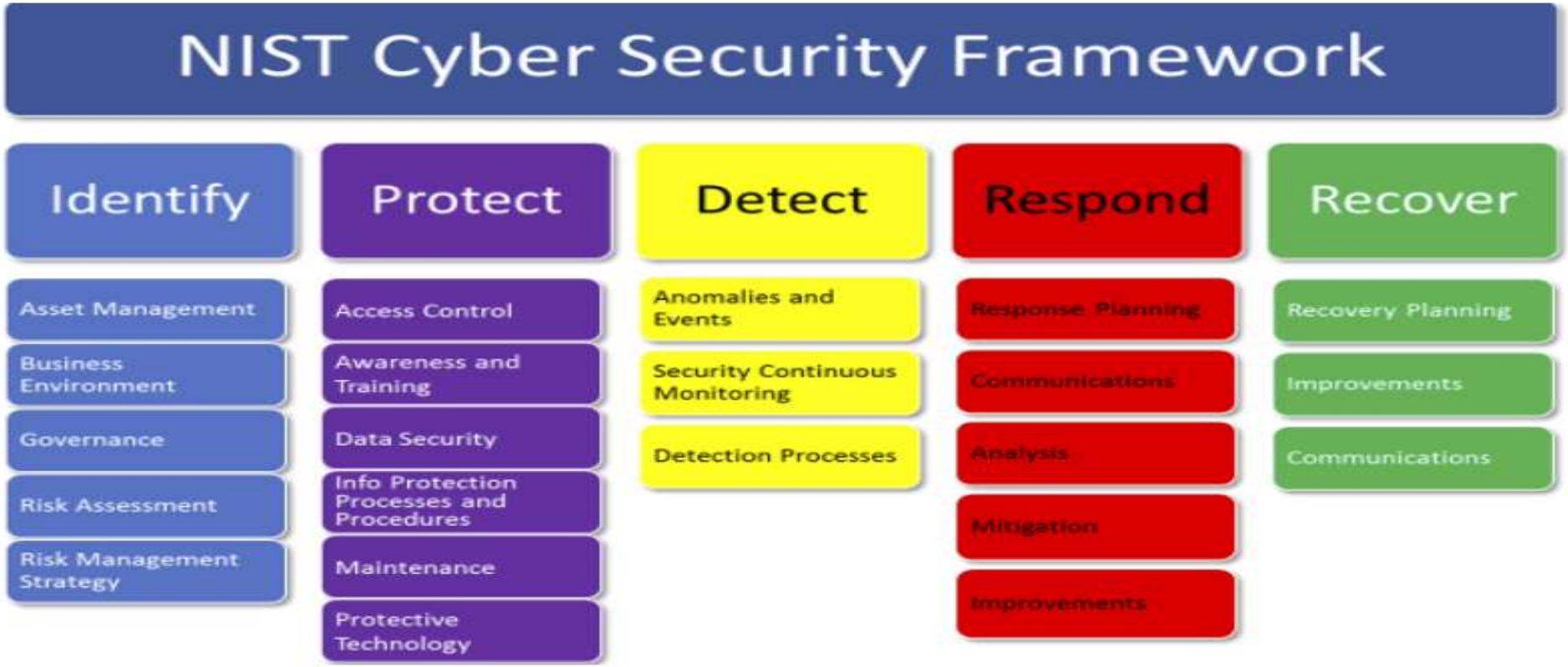


Focus on SIEM

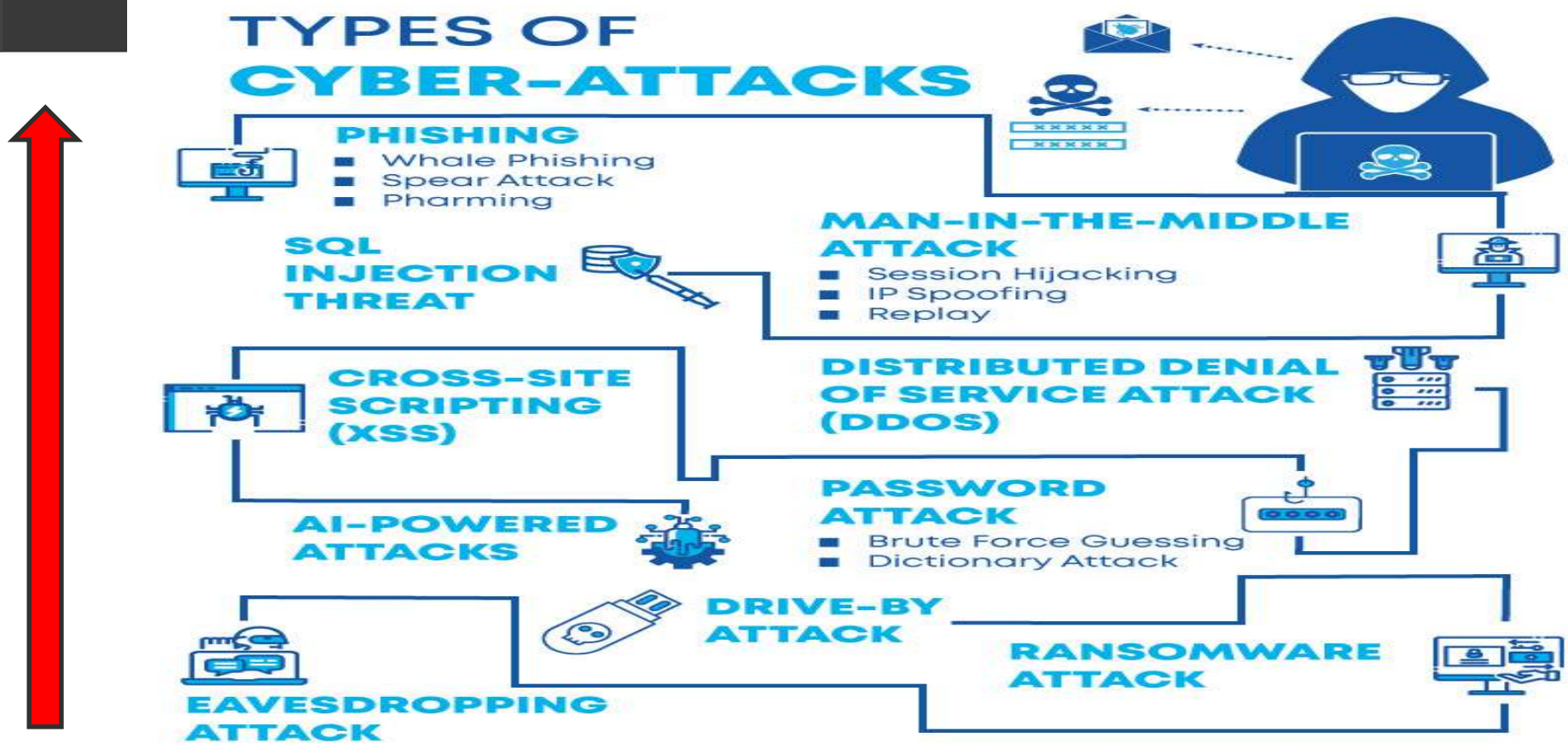


SIEM fits under Detect

https://securityaffairs.co/wordpress/58163/laws-and-regulations/nist-cybersecurity-framework-2.html



Why Cyber Security needed?



Difference between Info vs Cyber Security

Information Security : Security of Data at rest

Cyber Security : Security of data in-motion or in-transit

The cybersecurity foundation

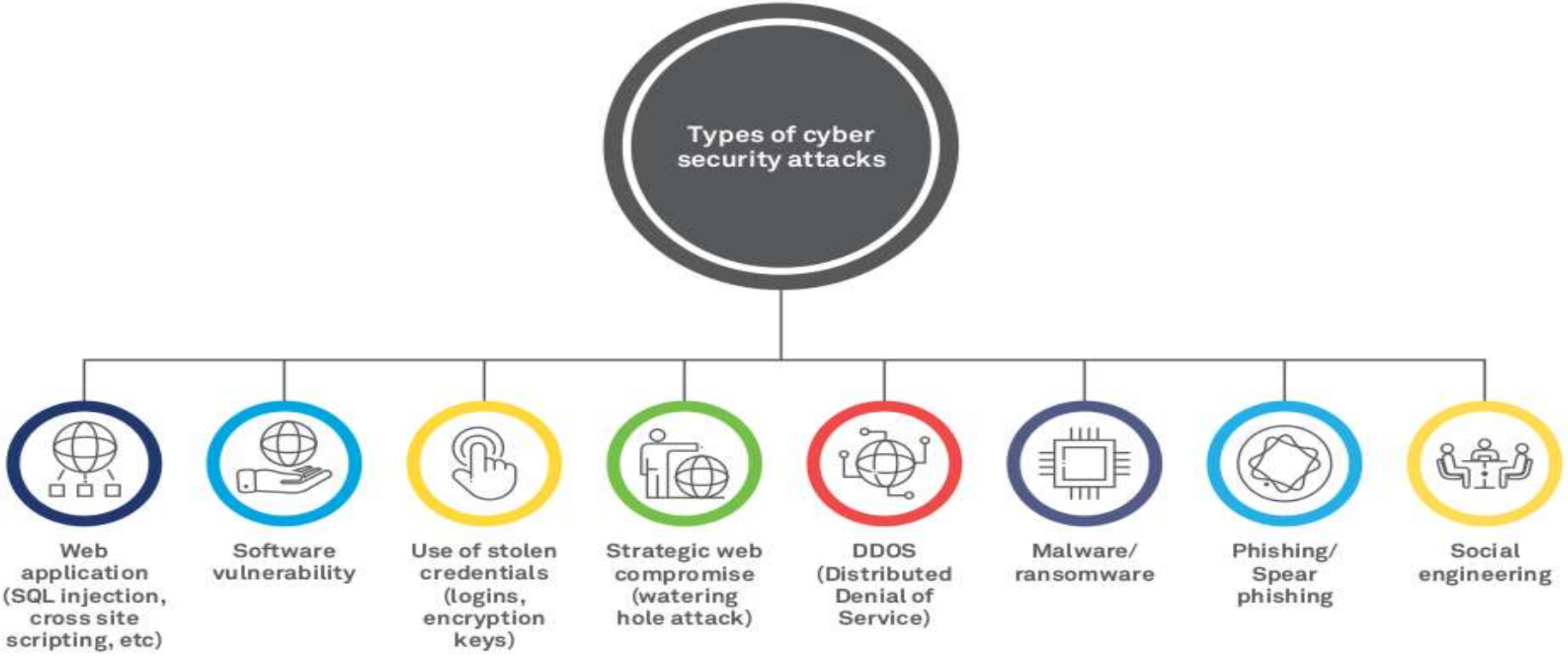
Security Principles

Confidentiality

Integrity

Availability

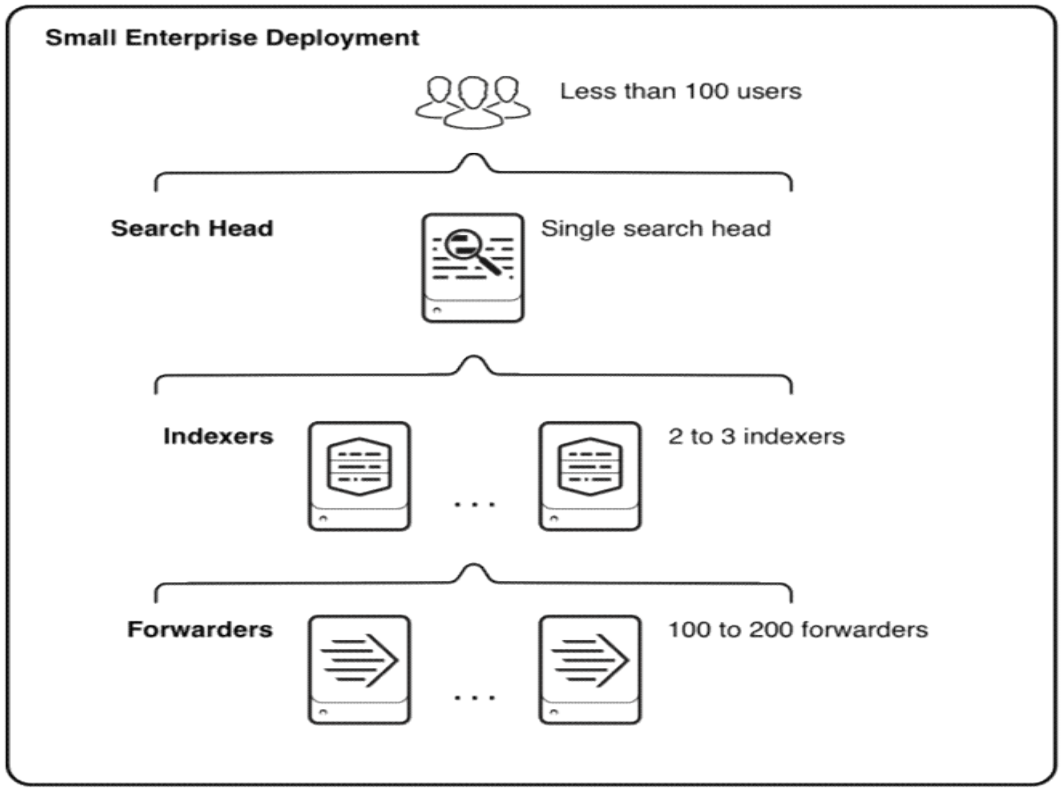
Cyber attack Techniques and Types



Attack Frameworks

1. MITRE ATT&CK Framework
2. MITRE CAPEC Framework
3. NIST
4. OWASP

FDP Lab Structure - Splunk

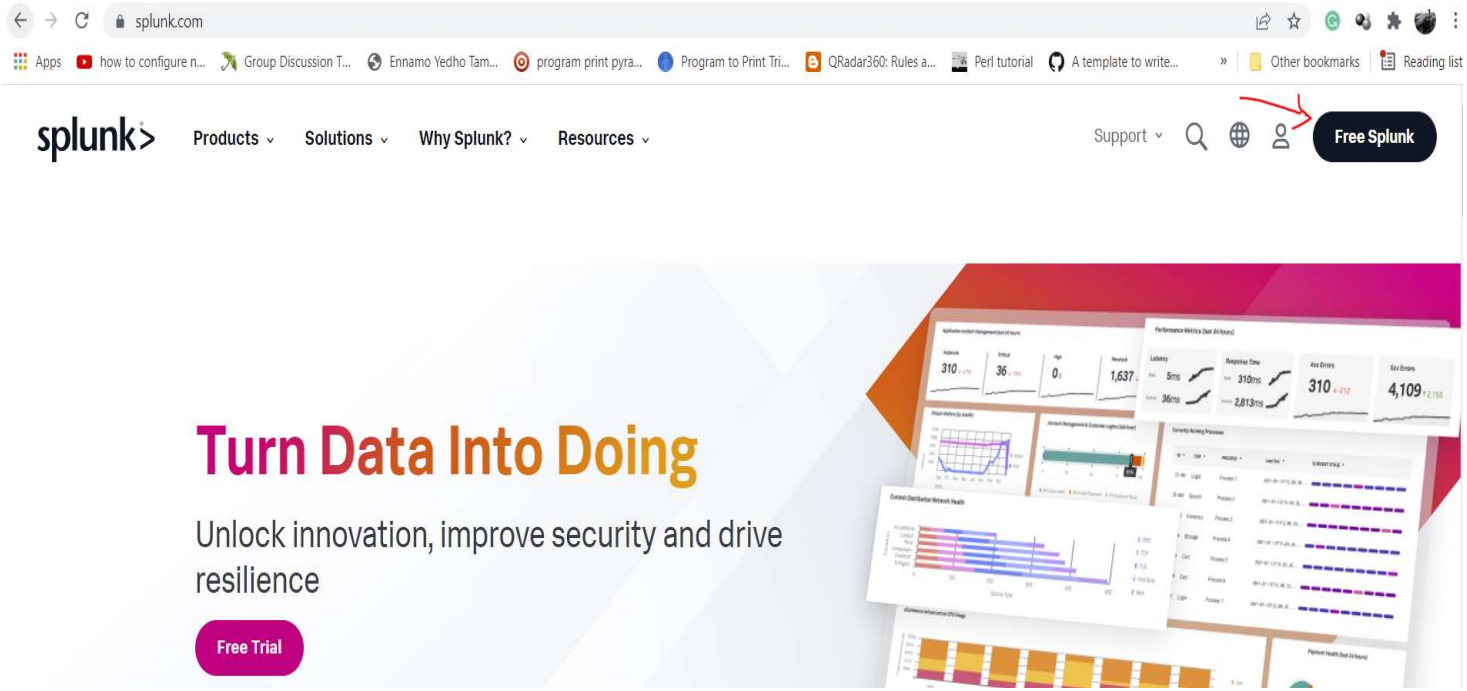


We will use AIO (All-in-one)

60 days trial version splunk

Download Splunk

* Visit www.splunk.com -> Click on Free Splunk -> Create account



Pre-requisites Or Good to have

Success is no accident. ...

Linux

Linux 101 Hacks Book https://www.thegeekstuff.com/linux-101-hacks-ebook

Network

TCP/IP Protocol Suite Book by Behrouz A. Foro uzan OR PPT

Database

Any database not limited PostgreSQL .. Revisit DDL, DML and DCL queries.

Regular Expression

https://regex101.com/

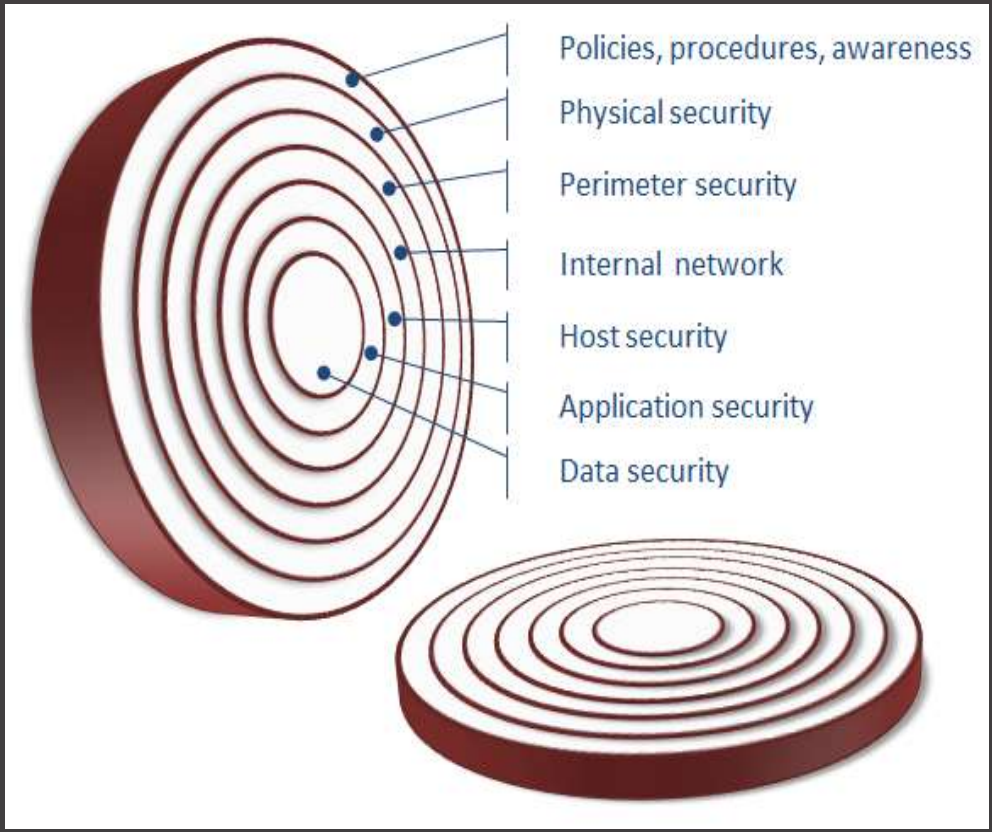
Important Devices

Linux, Windows, Firewall, Proxies, Router, Application logs etc.

Study Link

https://www.securitylearningacademy.com/
https://www.youtube.com/user/IBMSecuritySupport

Defense-in-Depth Strategy.

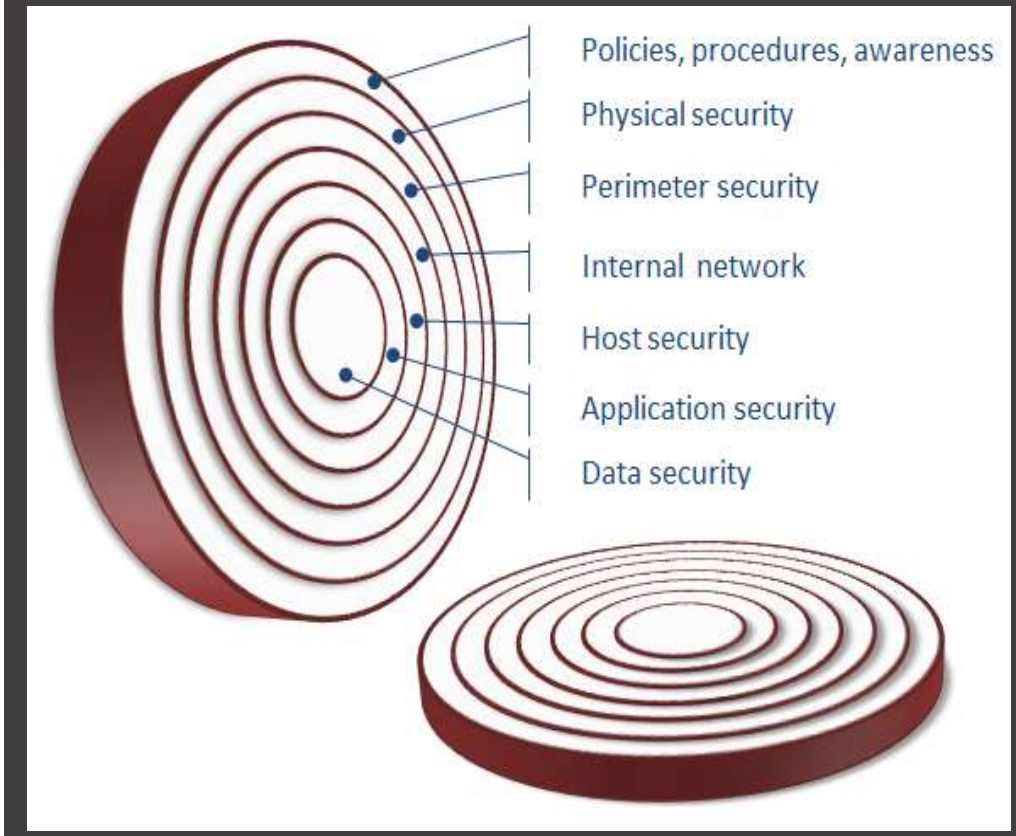


Multilayer defence strategy

1) Policies , Procedures, Awareness
→ Non Technical
→ Because Human is weakest link

2) Physical Security
→ Access control
→ Locks
→ Camera

Defense-in-Depth Strategy.

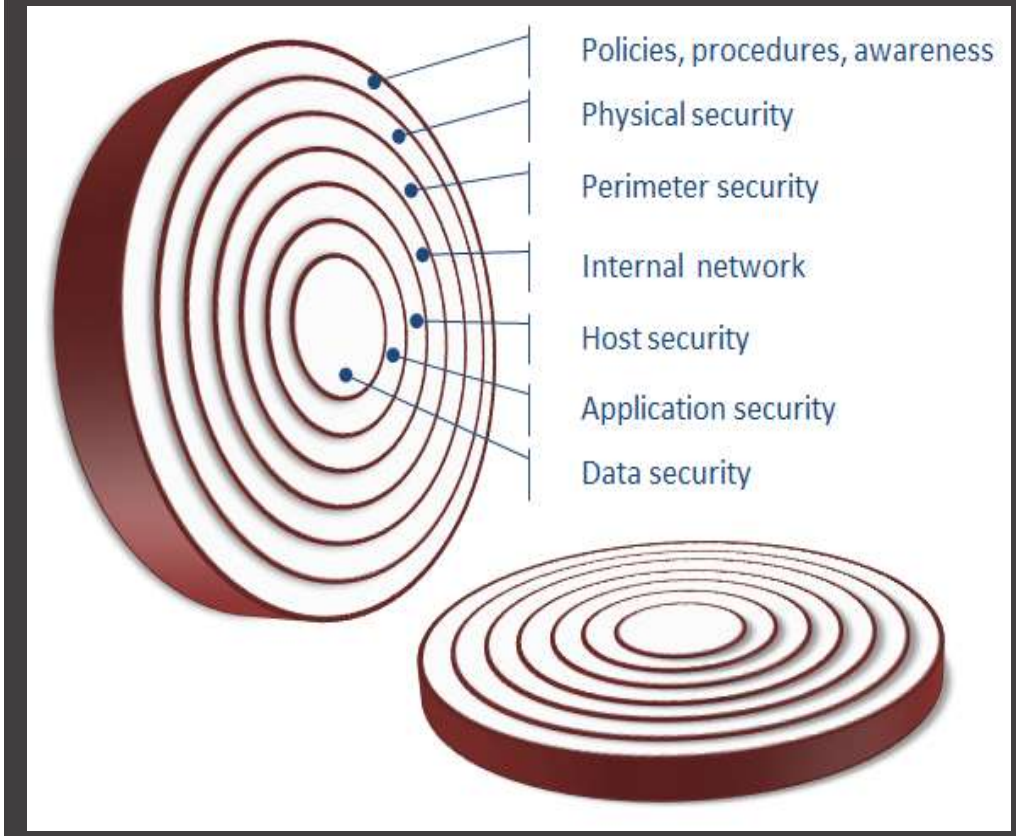


Multilayer defence strategy

3) Perimeter Security
→ Firewall, IPS, IDS
→ Segmentation VLAN
→ File permission, User access

4) Internal Network
→ Best practices - Routing Protocol
→ Control plain policing – Permit & d eny filter, QoS filter
→ Hardening – Disable unwanted ser vices, disable unwanted features.

Defense-in-Depth Strategy.

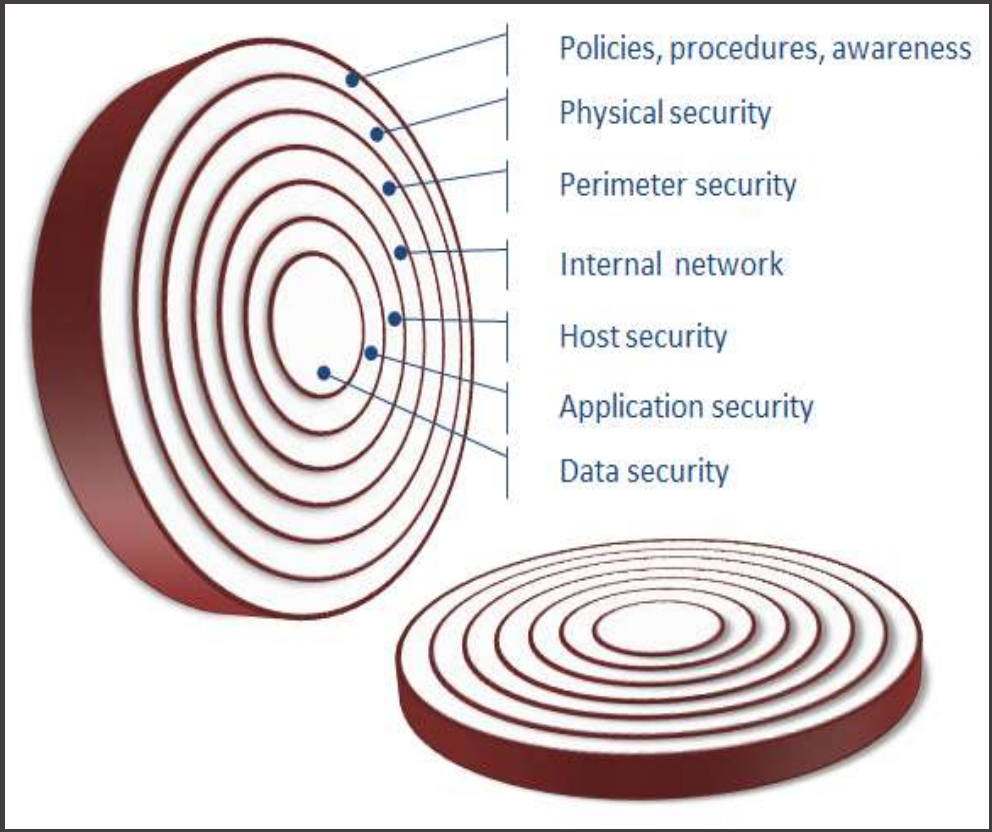


Multilayer defence strategy

5) Host Security
→ Antivirus
→ Password policies
→ Malware protection
→ VPN – remote access

6) Application Security
→ Application Robustness
→ Quality assurance testing
→ Broken software – open window for attacker
→ Keep up to date software

Defense-in-Depth Strategy.



Multilayer defence strategy

7) Data Security
→ Encryption
→ Backup
→ Monitor

ERIN

E : Events
R : Rules
I : Incidents
N : Notification

- Note : Right person should get notification about the incident via
  A) Email
  B) Ticketing system : using API
  BMC remedy, Service now, Jira, IBM Resilient etc.

- Normally when incident occurs
  L1 team → L2 Team → L3 / CIRT Team

Why SIEM?

Why SIEM needed?

1) Gather information at one place and help to monitor security posture of organisation
2) Detect suspicious behaviour
3) Detect problems before they become breaches
4) Monitor & enforce corporate policies
5) Reports : Regulatory compliances – PCI, HIPAA etc

What SIEM / QRadar does?

- Main functions

A) Collect logs from different endpoints like Firewall, IDS/IPS, AD, Antivirus, Wire less controller, Linux servers, windows servers, proxies etc.

B) Logging and reporting

→ Log user access

→ Track system changes

→ Monitor corporate policies and alert if policy violation happens

→ Provide reports for audit purpose

C) Correlation and Cross-correlation

→ Combine data from different sources

→ Identify Hidden threats

→ Reduce false positives

D) Real time alert generation.

What is SIEM (SIM + SEM)

- SIEM – Security Information / Incident & Event Management
- SIEM acronym is ”sim”

- SIEM tools provides real time alerts or risk to organization.
  In market there are so many SIEM products like
  A) IBM QRadar
  B) Arcsight
  C) LogRhythm
  D) Splunk etc……

Question?

Is Firewall, IDS, IPS, Antivirus are enough to protect malware?

Are you secure / compromised ?

Once you infected then attacker can

1) Remote control
2) Data extraction
3) Remote monitoring
4) Data destruction
5) Privilege escalation
6) Remote attack
7) Ransomware

Firewall, IDS/IPS, Antivirus not
Enough to protect from malware
Or from advance threats

SIEM Vendors – Gartner

SIEM Leaders:

- IBM Qradar
- Splunk
- Securonix SNYPR
- Exambeam etc

Figure 1. Magic Quadrant for Security Information and Event Management

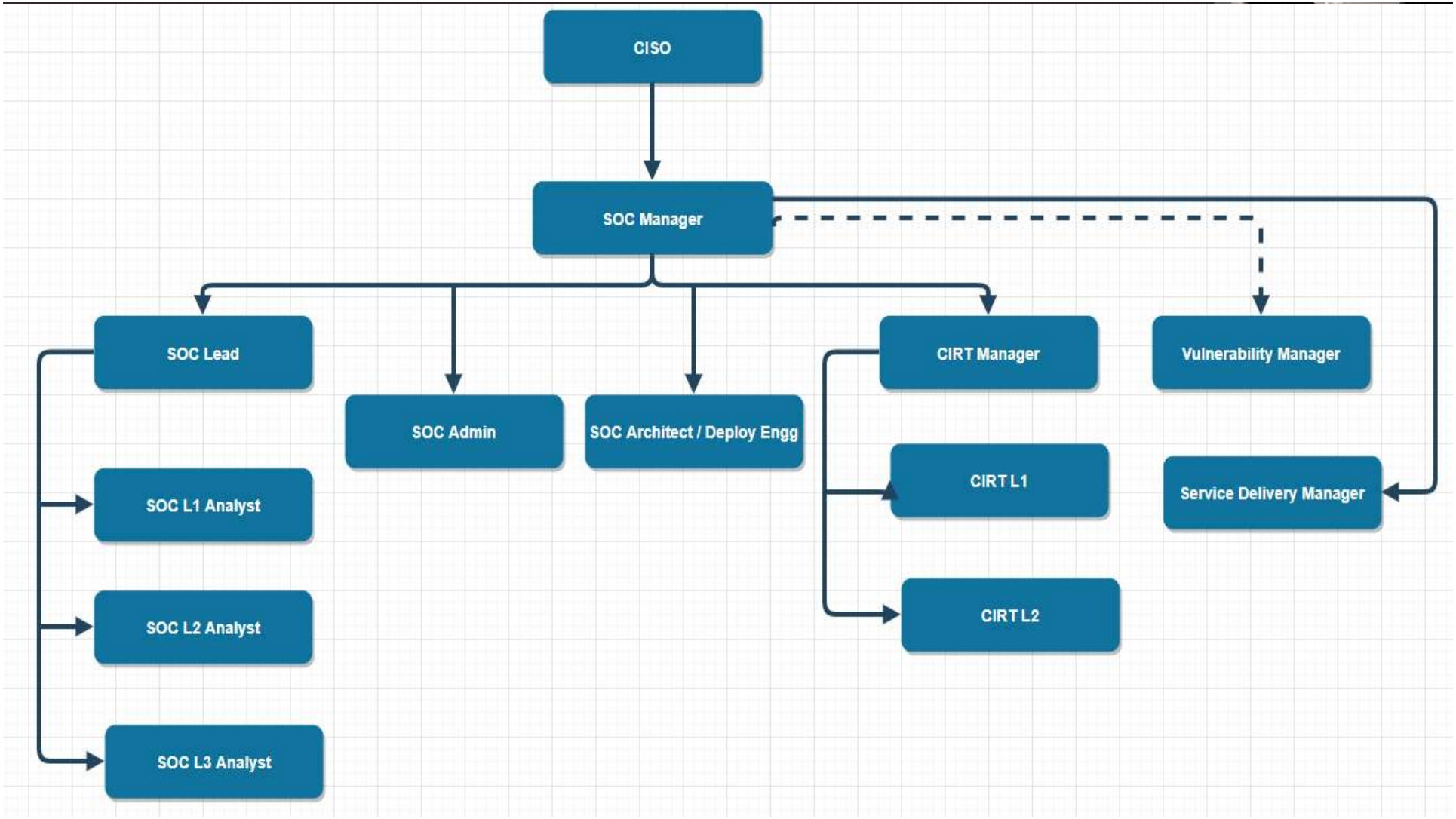
Source: Gartner (February 2020)

Roles

Splunk / Qradar is just product so focus on domain knowledge

Designation / Job Titles in Security Area

- Analyst L1
- Senior Analyst L2
- Lead Analyst / Level 3
- QRadar Admin
- Content Development Engineer
- Operational Engineer
- Professional services
- QRadar Engineer / Architect
- Vulnerability Manager
- SOC Manager
- Cyber Security Director
- CIRT L1
- CIRT L2
- CIRT Manager
- Red team
- Blue team
- Penetration tester
- Web Penetration tester
- Wireless Penetration tester
- Network Security Engineer
- Network Security Analyst


CISO
SOC Manager
SOC Lead
SOC Admin
SOC Architect / Deploy Engg
CIRT Manager
Vulnerability Manager
SOC L1 Analyst
CIRT L1
Service Delivery Manager
SOC L2 Analyst
CIRT L2
SOC L3 Analyst

Important Certification

- CEH / Security +
- CCNA / Network +
- RHCSA
- RHCE
- CompTIA Certifications (https://certification.comptia.org/certifications)
- CISSP
- OSCP
- OSCE
- CISM
- CISA
- CCSP

ERIN

E : Events
R : Rules
I : Incidents
N : Notification

- Note : Right person should get notification about the incident via
  A) Email
  B) Ticketing system : using API
  BMC remedy, Service now, Jira, IBM Resilient etc.

- Normally when incident occurs
  L1 team → L2 Team → L3 / CIRT Team

QRadar Source of Information.

Log sources

OS, Firewall, Proxy, Databases

Flow sources

Network listening, Net flow, Qflow

Vulnerability Scans

Qradar VM, Third party scanner like nessus, nCircle etc

Assets Information

Asset weight, Network hierarchy, manual info.

Threat Intelligence

IBM X-force, Threat grids etc

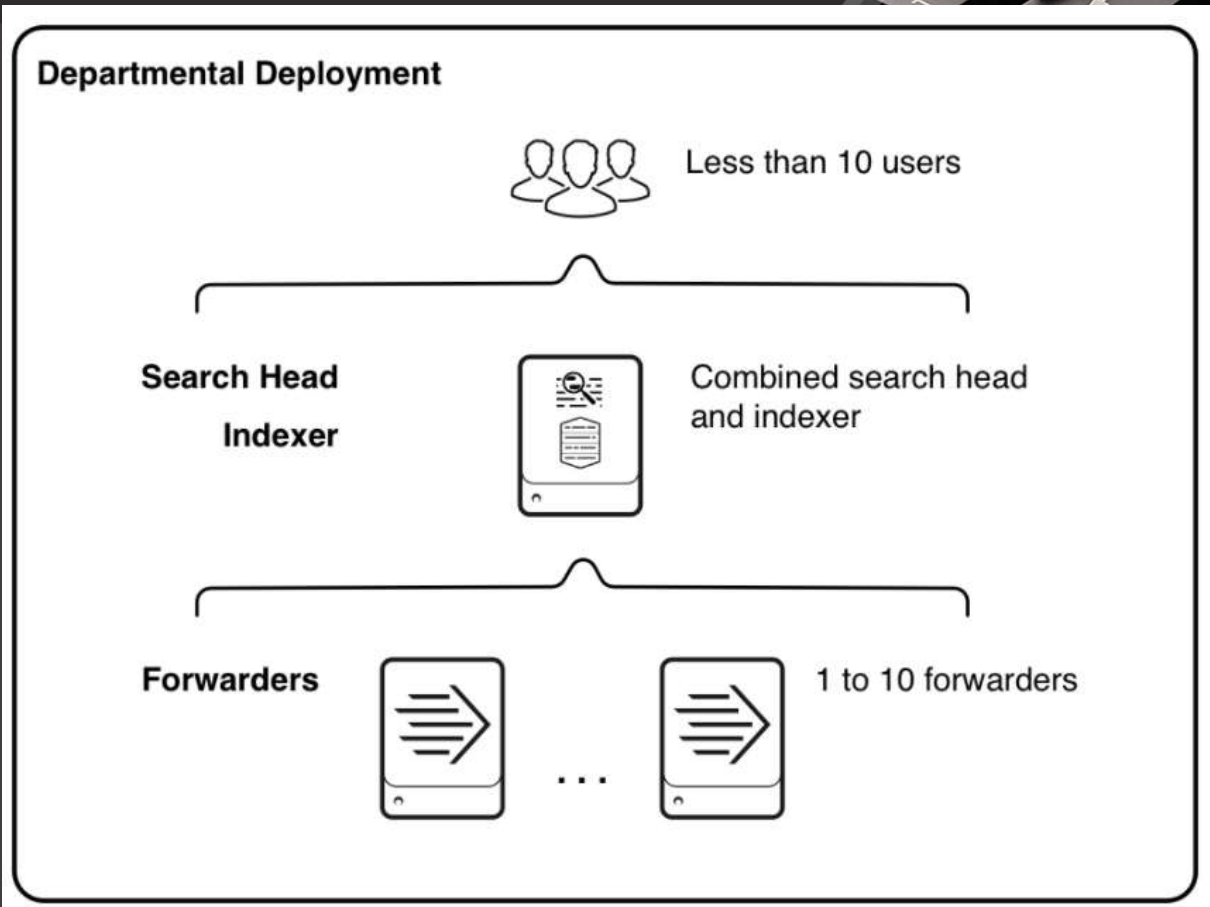
Reference watch list

HR feeds, Blacklisted, Manual input..

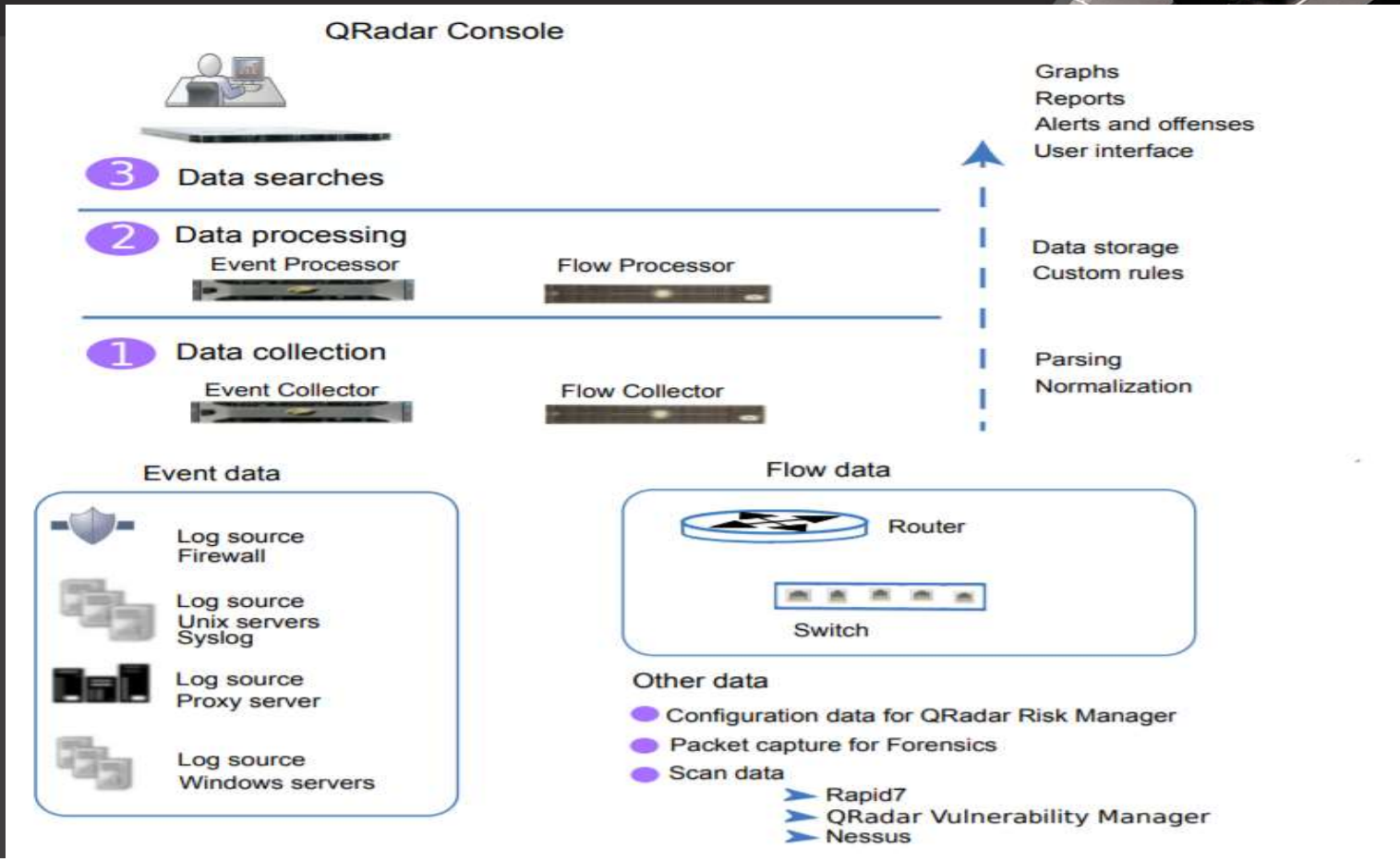
Splunk Architecture

3 IMP components:

1) Forwarders
2) Indexer
3) Search Head



QRadar Architecture



Ref: IBM Arch & Deployment guide

What is log source

- A log source is a data source that creates an event log.
- For example,
  - Linux
  - Windows
  - AD
  - Proxy – Cisco iornport or bluecoat
  - WAF – Imperva

Log Source : The endpoints from which we collect logs OR A log source is any external device, system, or cloud service that is configured to eith er send events to SIEM system or to be collected by your SIEM system using pull.

Methods to Collect logs

Types to collect logs in QRadar

To receive raw events from log sources, QRadar supports many protocols.

- **Push Method** : QRadar listen for events on specific ports.

For example Linux OS sends logs towards QRadar on port 514 using syslog/ rsyslog / syslog-ng.

- **Pull Method** : use APIs or other communication methods to connect to ex ternal systems that pull and retrieve events.

Example 1: In some cases like custom application logs we need to poll logs from endpoint using Log file i.e using SCP, SFTP etc.

Example 2: Suppose we need to collect logs using API after 10 min interval.

Install Splunk

Ingestion of sample logs

Reach out to us

- Whatsapp - +91 8087114770
- Mail me at pavaskarmahesh@gmail.com

Thank you