
SOC
XOXO XOXO XOXO
FUNDAMENTALS
ABHINAV SHARMA
//ABHINAVSHA007

The SOC and Its Roles :

The Security Operations Center is a centralized unit within an organization that deals with the security issues, incident and events.

1. Monitor :
    - continuous observation.
    - IDS / IPS
    - Early detection
2. Detect :
    - Confirming the security threat identified during monitoring.
    - IOC (Indicator of compromise)
3. Analyze :
    - Perform in-depth investigation to understand the security incident.
    - Examine infected systems
4. Respond :
    - Formulate a response plan based on findings .
    - Contain threat, mitigate impact, restore normal operation.

Key Functions Of A SOC :

Reactive Roles :

- Monitoring & Detection
- Incident Response
- Forensics Analysis
- Malware Analysis

Proactive Roles :

- Threat Hunting
- Vulnerability Management
- Security Awareness Training

Information Security Refresher :

CIA Triad :

1. Confidentiality :
    - Protection of sensitive data from unauthorized access.
    - Ensure Data is only accessible to theos with proper access.
2. Integrity :
    - Ensure that data remains accurate, complete, reliable and consistent.
3. Availability :
    - Ensure that resources are always available for use when needed.

AAA Framework :

1. Authentication : Verifies the identity of the user attempting to access the system (eg. pass, key etc).
2. Authorization : Access based on role , permission & privilege.
3. Accounting : tracking and recording activities within a log (login attempt, resources access, audit logs)

Vulnerability :

- Weakness in the system, network or a product.
- Can be exploited to compromise the CIA

Threat :

- Any potential Danger to info or system
- Malware, phishing, DOS.
- Takes advantage of vulnerability.

Risk :

- Likelihood of a threat exploiting a vulnerability.
- Potential for loss or damage when threat occurs.

Logs :

A record of events or actions that have occurred within a system.
Used for Monitoring and doubling security incidents.

Security Events :

- Any observable occurrence that has a potential significance for security.
- Any incidents are events but not all events are incidents.

Security Incidents :

- Any occurrence that actually jeopardies info security.
- Consists of A violation of security law, security policy, procedure or acceptable use.

Security Controls :

1. Defense In Depth :
   - Strategy of Layered security.
   - Multiple barricades to threat.
2. Administrative Control :
   - Security Policy
   - Change management Plan.
   - Incident Response Plan.
3. Technical Control :
   - Firewall, EDR
   - IDS
   - 2 Factor Authentication.
4. Physical Control :
   - Access Control System
   - Surveillance Camera
   - Biomatrices, guard, fencing.

Security Control Function :

1. Preventive Control -
   - Eliminate or reduce the chances of a attack succeeding.
   - ACLs, firewall, EDR, IDS.
2. Detective Control -
   - Identify and record attempted or successful intrusions.
   - IDS, SIEM, Logs , surveillance camera.
3. Corrective Control -

- Eliminate or reduce the impact of an intrusion.
- Backup , IR Plan, Patch management.

4. Deterrent Control -
   - Discourage Intrusion attempts
   - Physical barriers, signs, temper seals.
5. Compensating Control -
   - Act as an alternative mean for a physical control
   - Network Segmentation, data masking.

A single device might act as multiple controls , eg : Camera - Detective, Deterrent, Physical.

Risk Control Strategies :

1. Risk Transference :
   - Shifting responsibility to a third party.
   - Security insurance , Cloud service providers.
2. Risk Acceptance :
   - Acknowledge and tolerate the risk.
3. Risk Avoidance :
   - Proactively eliminate or avoid exposure to risk.
   - Limiting the type of data stored on a server
4. Risk Mitigation :
   - Reduce the likelihood or impact of a risk
   - Implementing patch management.

Security Policies :

1. Acceptance Use Policy (AUP) :
   - What is and is'nt allowed within the org.
   - Bring your own device(BYOD)
2. Password Policy
3. Data classification Policy
4. Change Management Policy
   - Planning and implementing change to a system or process.
5. Disaster Recovery Policy

SOC Models :

1. Internal Soc :
   - Implemented By the Organization.
   - Requires Investment in Training.
2. Managed Soc :
   - 3rd party provider for security operations.
   - Subscription based SLA's (Service level agreement)
3. Hybrid Soc :
   - Mix of both.
   - Incident Response, forensics , malware , call in the expert as neened.

Event Management :

1. Collection , Normalization, Analysis. (conducted by devices and systems).
2. Logs, Alerts, End Points (Firewall, IDS, antivirus, EDR, Webserver).
3. Identifying abnormal or suspicious activities (Rules and alerts on behavior known malicious artifacts)

Incident Management :

1. Incident Identification (Detection Mechanism, Event management)
2. Incident Classification (severity, Impact nature)
3. Incident Investigation (Gather evidence, determine scope)
4. Incident Containment (Prevent further escalation)
5. Incident Eradication (Remove Evil)
6. Incident Recovery

Detection outcomes :

- False Positive : Incorrect Identification of activity.
- True Positive : Correct Identification of a real security incident,
- False Negative : Failed detection of real security threat,
- True Negative : Correct Identification of real bening activity.

SOC Metrics :

A quantitive measure that provide insights into the performance, effectiveness, and effectiveness of SOC.
They help in assessing how well the soc is detecting, responding, mitigating security threats and as well as how are they managing the response.

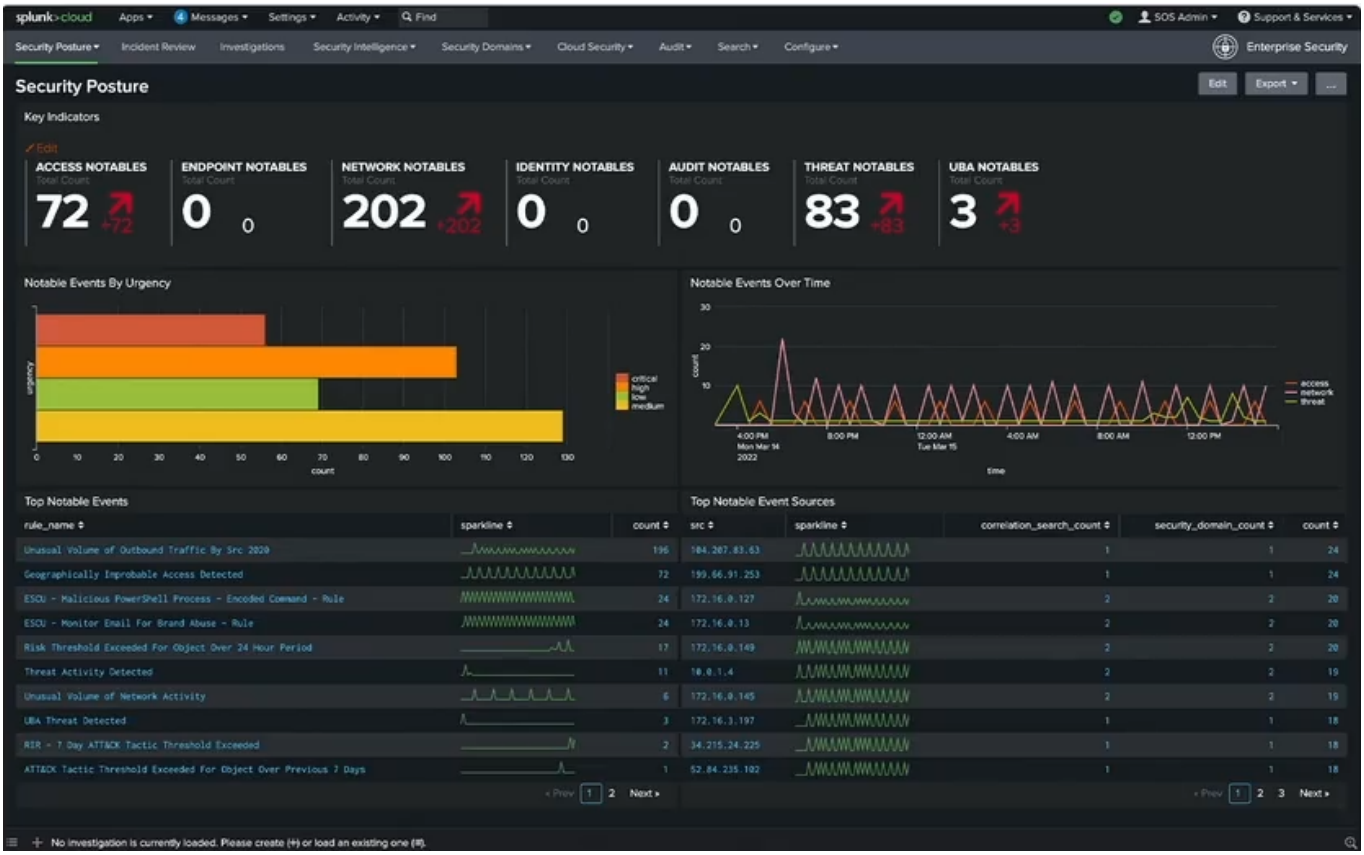
1. Mean Time To Detect(MTTD) - MTTD ↓ = fast detection.
2. Mean Time To Resolution(MTTR) - MTTR↓ (time resolve an incident) = More efficient
3. Mean Time To Attend 4 Analysis (MTTA4A) - MTTA4A ↓ = Reduce Response Latency
4. Incident Detection Rate - ↑ rate = better visibility for monitoring.
5. False Positive Rates (FPR) - ↓ rate = more accurate detection.
6. False Negative Rate (FNR) - ↓ rate = more accurate
7. Key Risk Indicator (KRI) - measurable values to asses risk.
8. Service Level Agreements (SLAs) - Agreement between SOC team and the SOC Client , individual response time , lever of service and performance.

SOC Tools :

1. SIEM (Security Incident & Event Management) :

==LogRhythm ,Splunk, IBM Radar, ==
A SIEM serves as a platform for collecting, corelating and analyzing security event data in real time.
Aggregate logs generated by all over technologies and then we can implements advanced analytics to identify patterns or abnormalities in collected data.

- log management.
- Real Time Monitoring
- Alert 4 notification
- Incident Response
- Dashboard reports and visualization
- Threat intelligence Integration.

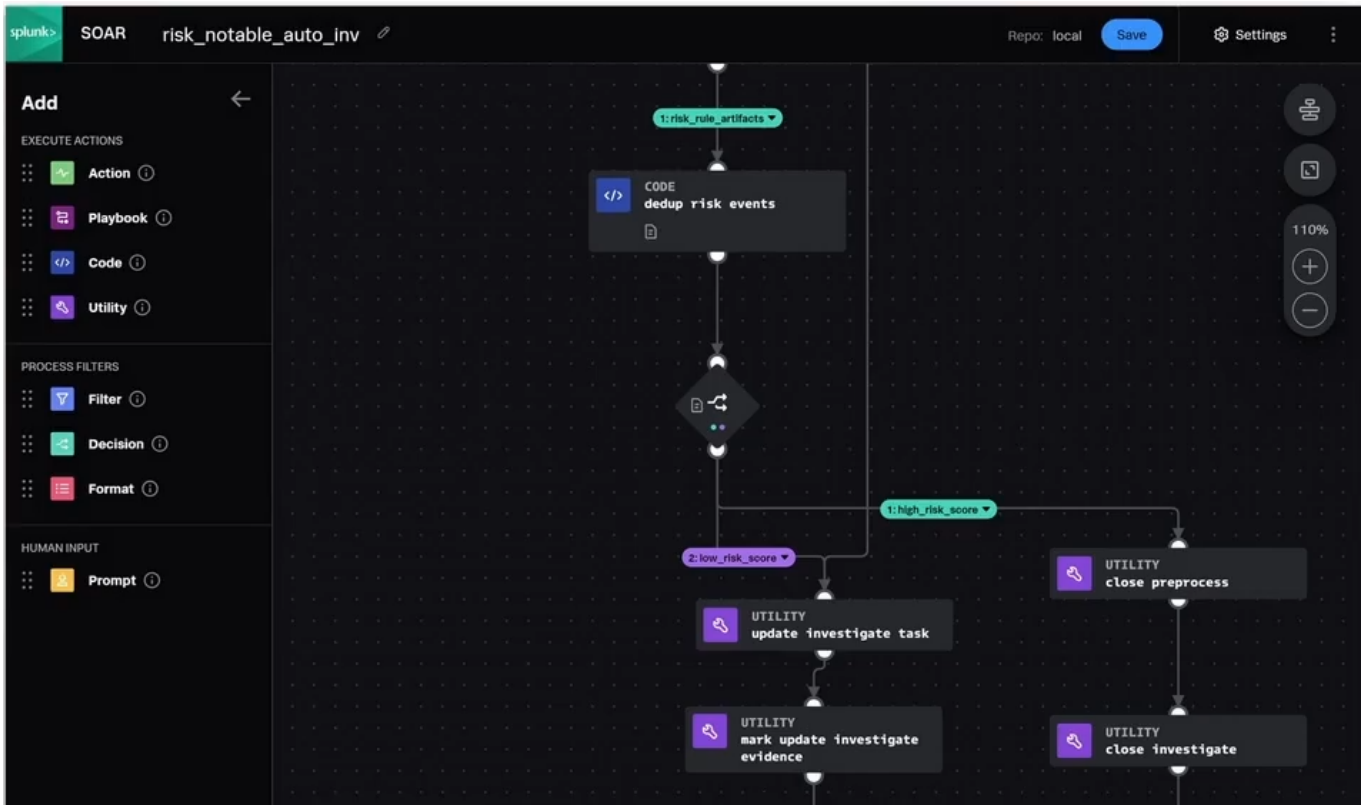


2. SOAR (Security Orchestration & Automated response) :

Splunk SOAR, IBM Qradar, Tines, LogRhythm, Blink

SOAR Platforms are designed to help SOC teams manage and respond to security incidents more effectively by automating respective tasks, orchestrating workflow across different security tools.

- Orchestration (workflow, collaboration) (we can automate siem, acls. firewalle etv)
- Automation (Alter Triage, Artifact collection, Data enrichment)
- Incident Response (Access & Prioritize)
- Integration (TIP's, EDR, Firewall etc)
- Analytics 4 Intelligence
- Reports (dashboatd)

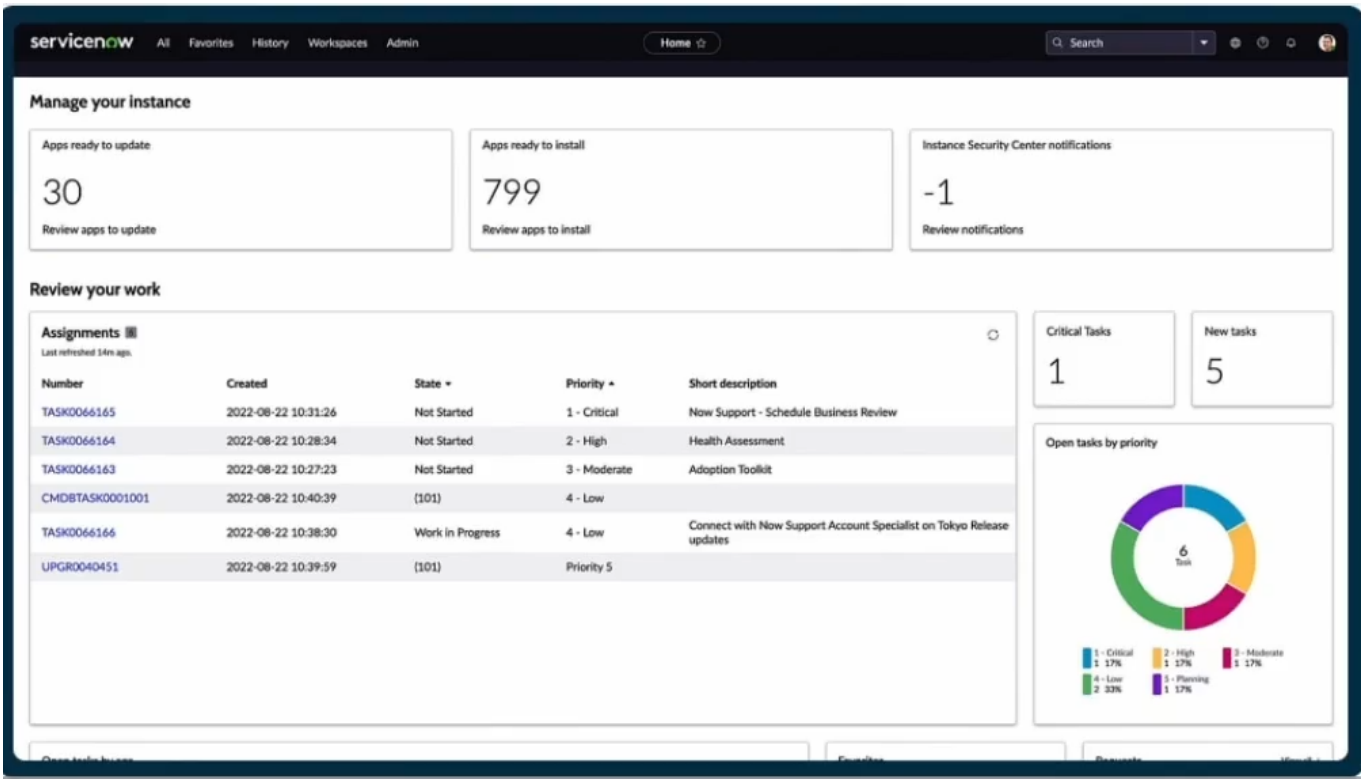


3. Incident Management Tool :

Atlassian, Service now,freshwork,ONPAGE

Tools used for detection analysis and specifically resolution of security incidents.
Provides a centralized platform for teams to collaborate and contribute and manage incidents.

- Incident Ticketing
- Alert Management
- Workflow Automation
- Collaboration

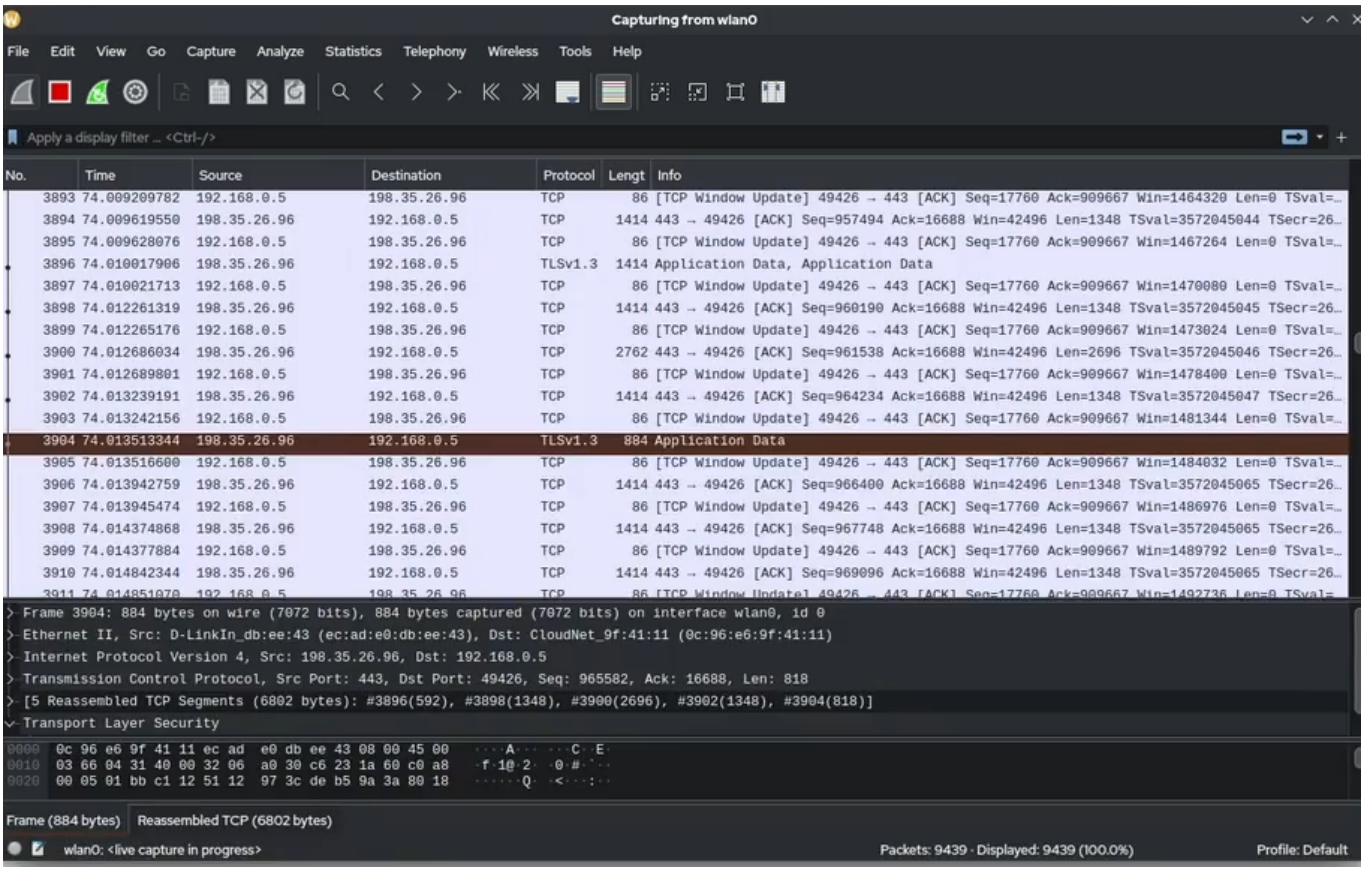


4. Network Security Monitoring(NSM) :

SUNIKATA, SNORT, NAGIOS, Wireshark, Zeek

Detectors for network related threat vulnerabilities, used to monitor network traffic , analyze network behavior for incident potential incidents in real time based on rule matching or behavior matching.

- Packet Capture & Analysis
- Network Traffic Analysis(Statical, ML , Behavioral)
- Incident Detection(sign based, Anomaly,)
- Integration with SIEM



5. IDS/IPS :

SNORT, SURICATA, ZEEK

Designed to monitor network traffic, detect potential security events and take actions to mitigate and prevent unauthorized access to malicious activities.

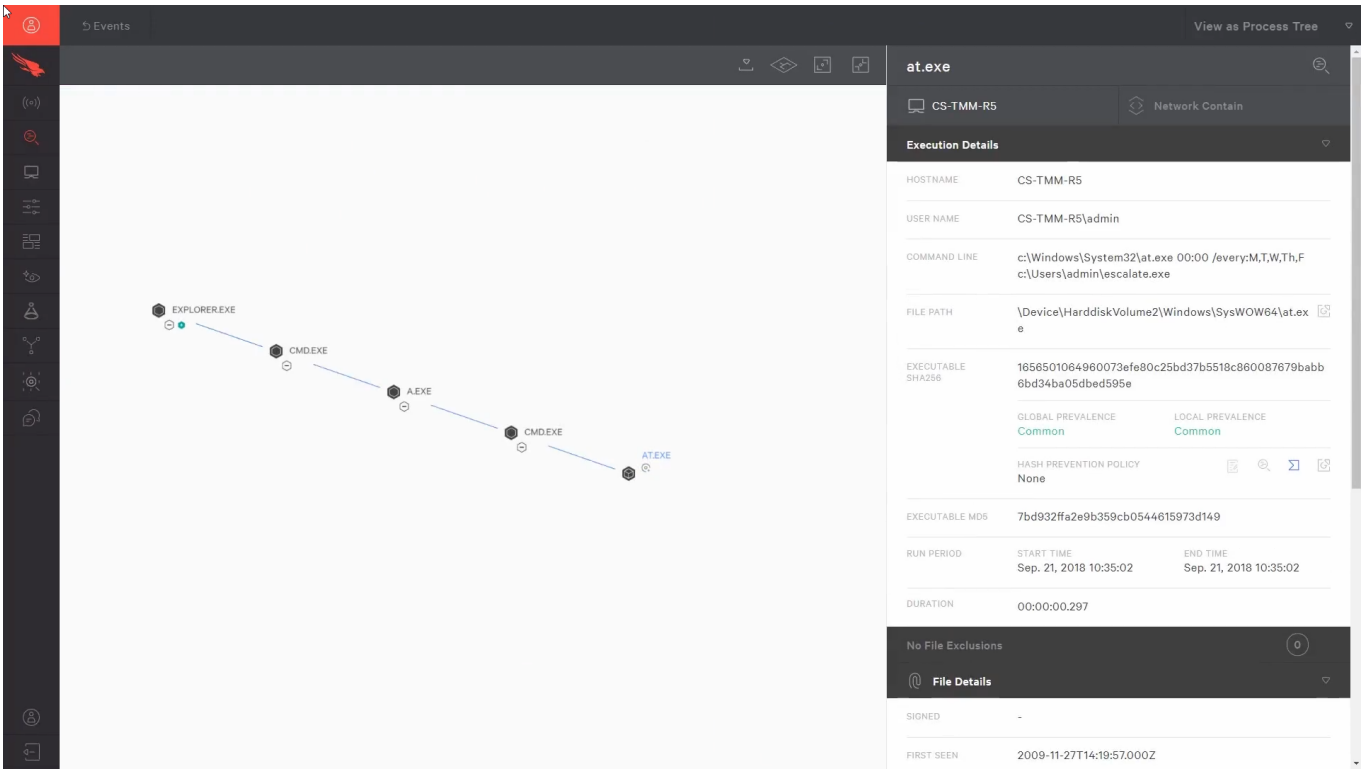
IDS - Passive or active monitoring (Designed to detect specifically) and generate alert based on Pre-defined rules.
IPS - Used to prevent attacks and is build upon IDS capabilities to actively block and prevent threat in real time.

IDS & IPS Both have Logging & Monitoring.

6. Endpoint Detection & Response (EDR) :

crowdstrike, SOPHOS, CARBON Black, Sentinel One

- Specifically focus on protection of End point devices (Laptops, servers, desktops, mobiles)
- Typically deployed with an agent that sits on the endpoint which provides organization with single point of glass capacity to detect, investigate and respond to security intendent at endpoint level.
- Real Time Endpoint monitoring
- User Entity Behavior Analytics (UEBA)
- Threat Detection & Prevention
- Intendent Investigation
- Remediation Response.
- Integration with SIEM



7. Firewall :

paloalto, SONICWALL, PFsense,JUNIPER Network. , FS, Cloudflare

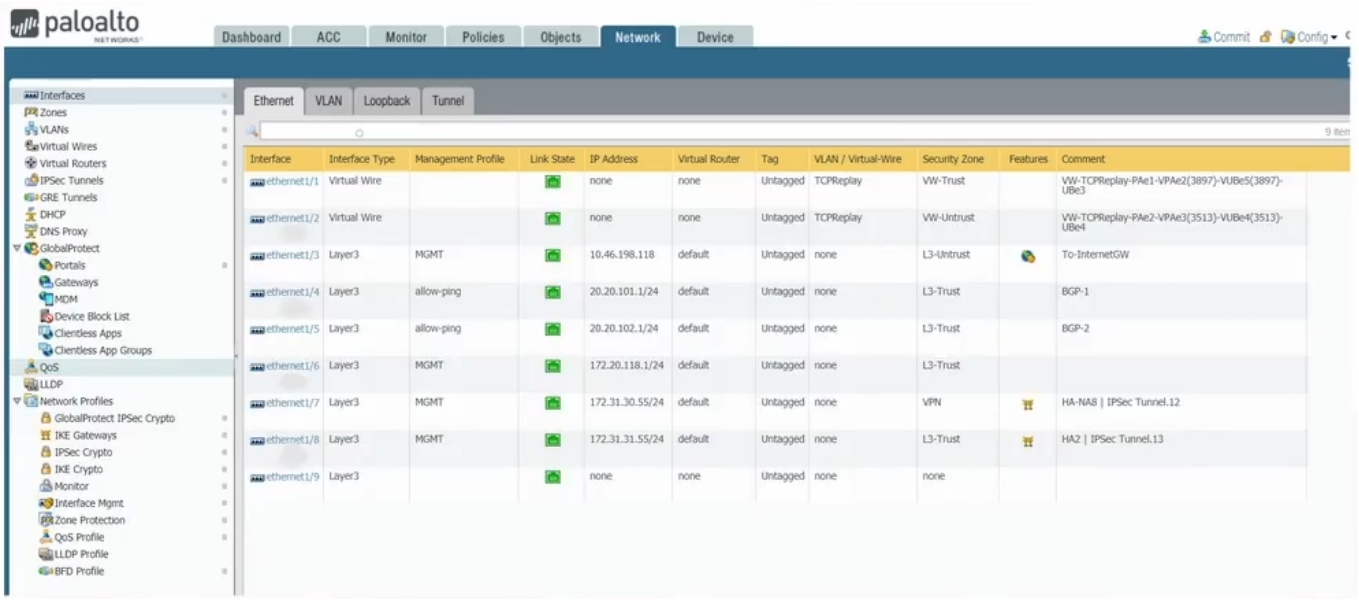
Firewall :

- A security device that monitors and controls incoming and outgoing network traffic based on predefined security rules .
- It Establishes a barrier b/w a trusted internal network and untrusted external network.

Functionality :

- Filter based on IP Addresses, Port, protocol.
- Implements basics policies using packet filtering.
- Stateful Inspection : uses state of active connection to death , which packet to allow

1. Network Firewalls -
   - Examine Packets
   - Layer 3
   - Make Decision based on rule
2. Next - Gen Firewall -
   - Statefull Packet genration
   - Deep Packet Inspection
   - Layer 7
3. Web Applications Firewall -
   - Inspect HTTPS traffic
   - Protect web apps from attacks
   - Layer 7



8. Threat Intelligence Platform (TIP):

openCTI, MISP Threat Shring, Maltego, Recorded Feature

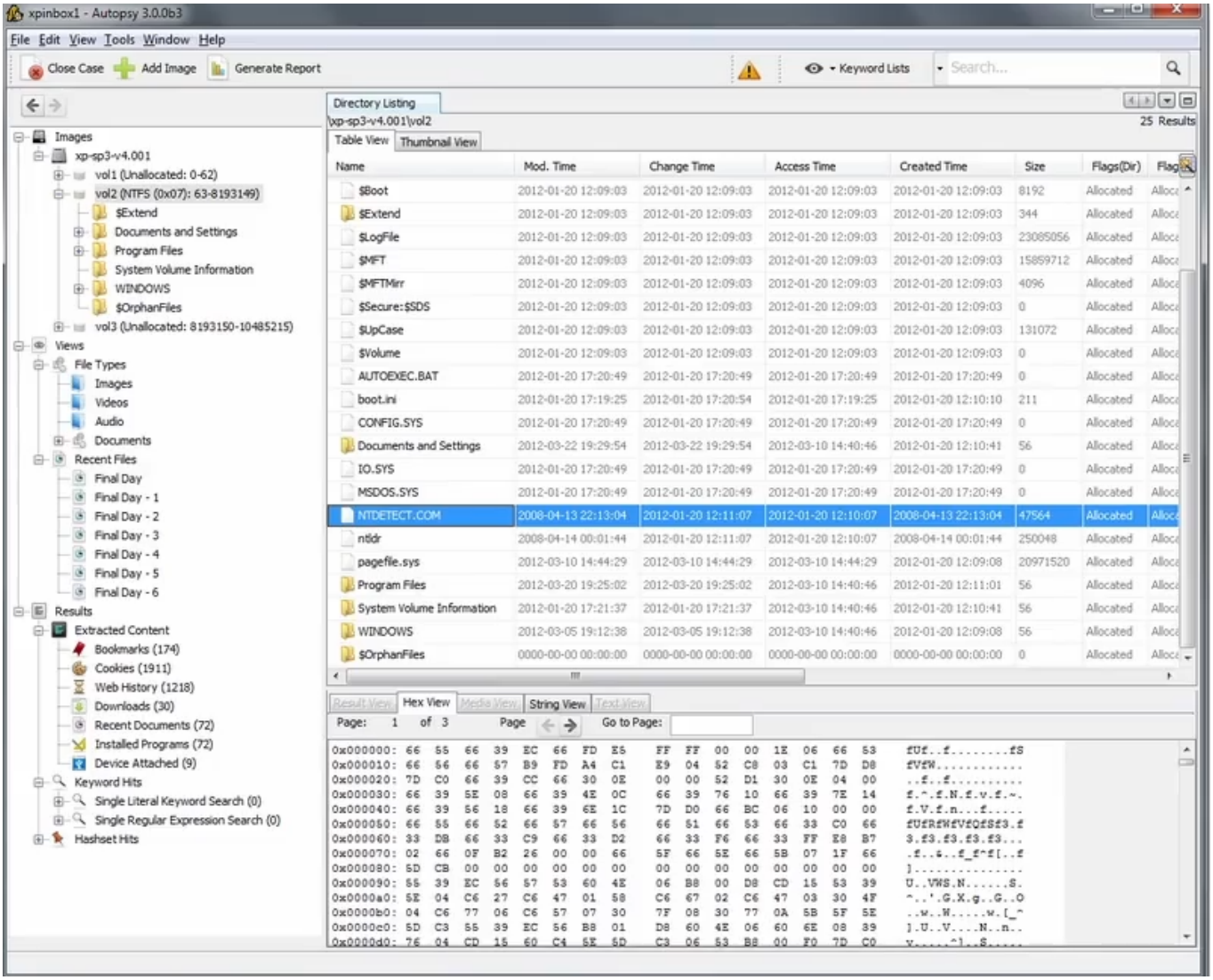
And these are designed to aggregate, analyze and operationalize threat intelligence data to enhance our defenses and improve threat detection and response capabilities.
It can be collected data from fields like : commercial fields, open source fields, government agencies.

- Data Aggregation and Enrichment
- Indicators of Compromise (IOCs)
- Normalization and Standardization
- Integration with SIEM

9. Forensics Analysis Tools :

==Autopsy, Encase, EZ Tool, ==
Special Softwares designed to collect, analyze and interpret digital evidence from computer, systems or networks or,storage devices for the purposes of forensic investigations.

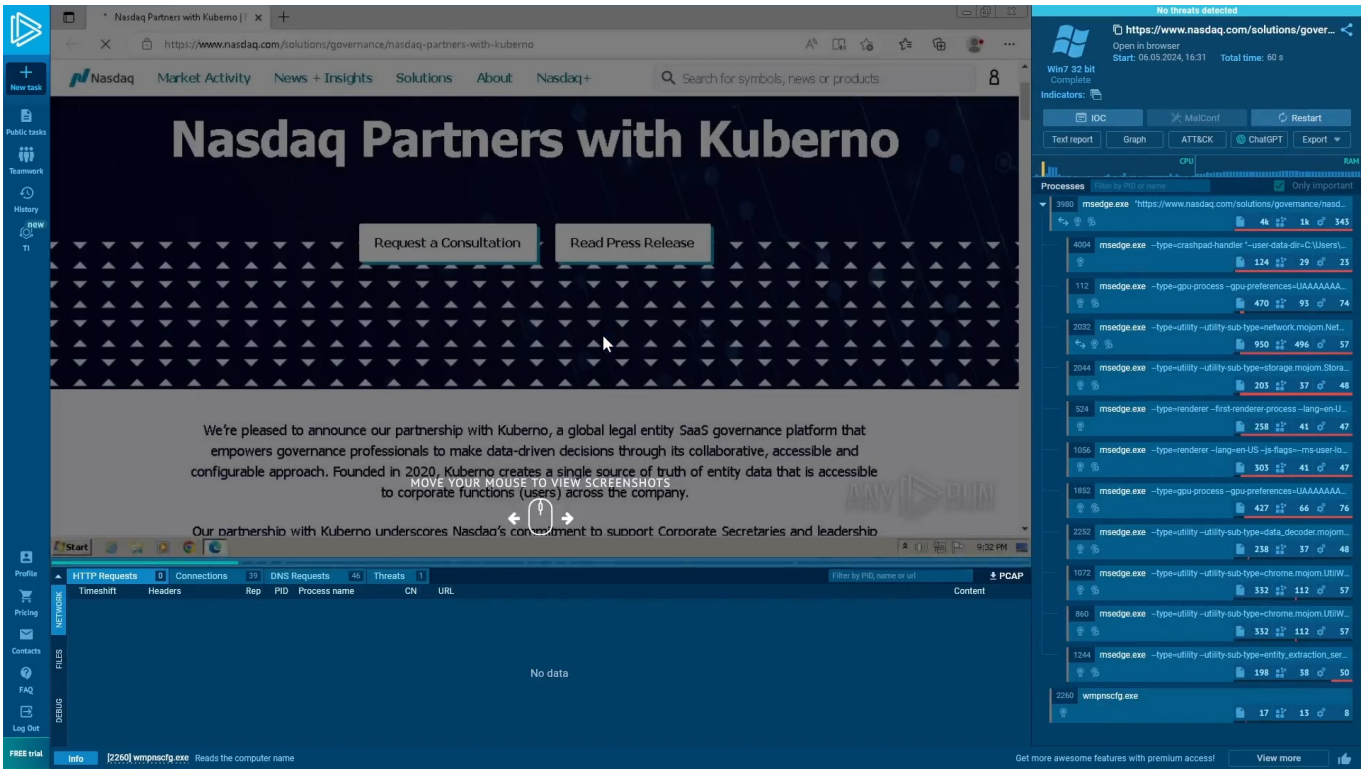
- Data Acquisition and Imaging
- File System Analysis
- Memory Forensics
- Registry Forensics
- Network Traffic Forensics



10. Malware Analysis Tool :

AnyRun, Hybrid Analysis, cuckoo sandbox, joe sandbox, ghidra

- Dynamic Analysis
- Static Analysis
- Behavioral Analysis
- Signature & Pattern Matching (known data)
- Integration with TIP's



Common Threats & Attacks :

1. Social Engineering :

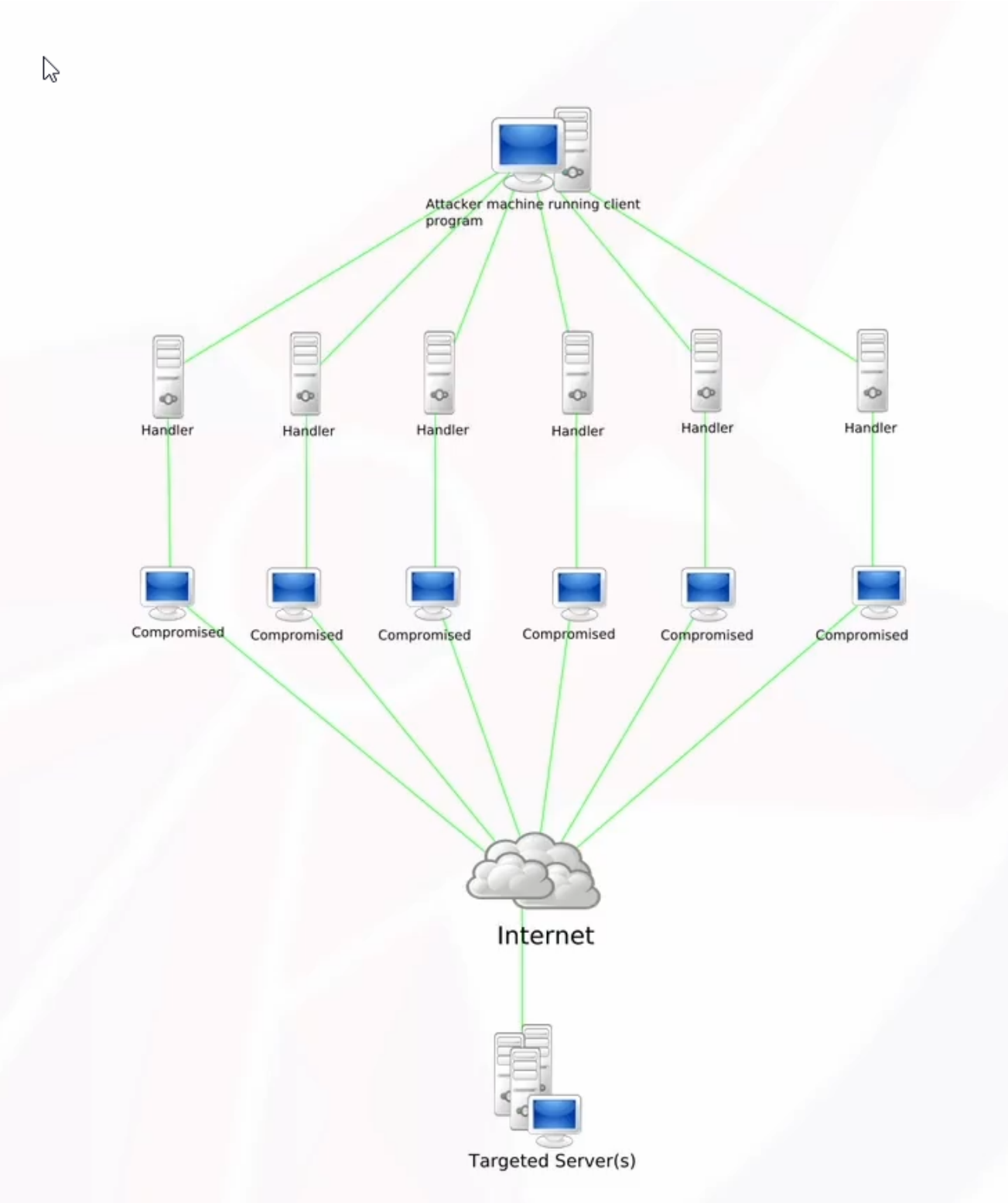
Exploit the human side of cybersecurity rather than any kind of technical vulnerability. (Human Hacking).
And a common goal here is to gain some sort of unauthorized access to a system, or exfiltrate some sort of data, or gain some sort of user credential that can

- Phishing : And phishing involves sending some sort of deceptive email or a message to someone, and appearing to be from some sort of legitimate source like a bank or a trusted Organization.
- Spear Phishing : It is a special Types of Phishing where the attacker is going to tailor their message specifically for an Individual or an organization.
- Whaling : spear phishing which specifically targets, high profile individuals within organization..
- Vishing - Or voice phishing, when the attacker calls someone over the phone and attempts to trick them into providing sensitive information.
- SMiShing - SMS Phishing , is an attack conducted through text messages or SMS messages.
- Quishing - QR code phishing.

2. Malware :

malicious software that's designed to harm or exploit an organization.

- Worm : And a worm is a malicious program designed to replicate itself and spread (Self Replicate, Infect & propagate)
  Eg - Stuxnet - highly sophisticated worm discovered around 2010, it was specifically targeted on SCADA systems used in industrial environments and particularly to attack, perticularaly to target Iran's nuclear program.
  Blaster - Ransomeware
- Spyware/Adware : These are the type of malware that either covertly monitor user activity or display unwanted advertisements, respectively.
- Trojan : Named after the famous Trojan horse from Greek mythology. As the name suggest these malwares disguise themselves as legitimate program to deceive users into executing it. (RAT - remote access trojan)
- Botnets : botnet is a network of compromised devices that use a central command and control server.



- Ransomware : malware that's designed to encrypt file on a victim's computer or within a network.
- Fileless Malware : Memory based Malware, it operates within memory and is able to execute and operate without any trace, evade detection & Logging [Living Of The Land]. It generally uses PowerShell scripts, WMI, Code Injection

3. Identity and Access Compromise :

It is also known as Identity theft or Account take over.

- Information Regarding Username, password, SSN, PII
- Impersonation, fraud, theft

4. Insider Threat :

It refer to the risk that an organization faces by individuals from within that organization, or someone who has authorized access to sensitive information.

- Current or former Employees
- Contractors
- Partners
  Types :
- Current or former employee
- Contractors
- Partner

Types : Malicious, careless, compromised

5. Advanced Persistent Threats (APTs) :

Sophisticated Cyber Groups cyber groups that are highly orchestrated and highly skilled and often well funded.

- Highly skilled, well funded adversaries
- Sophisticated
- Persistent (Long-term, quiet, and undetected access)
- They typically have strategic objectives. (espionage, or steal intellectual, property, or sabotage, or cause some sort Strike or disruption to critical infrastructure)
- https://www.crowdstrike.com/adversaries/ : For example, CrowdStrike uses a naming convention called Falcon Intelligence to identify APT groups.
- https://www.mandiant.com/resources/insights/apt-groups
- Other Good frameworks would be **Mitre.org** or OpenCTI check them out.

6. Denial Of Service Attack :

- Disrupt the availability of systems
- Flood of traffic and requests to Exhaust a system's resources and bandwidth
- Intentional or accidental
- Distributed Denial-Of-Service (DDoS)
  - Utilize multiple compromised systems
  - By using multiple devices and compromised an attacker can amplify their attacks.

7. Data Breaches :

- Data exposure, theft, or compromise (occurs when sensitive or confidential information is disclosed)
- PII, credentials, financial records, IP.
- Malicious actions and human error (Misconfiguration, Inadequate security controls)
- Reputational damage, regulatory trouble

8. Zero Days ;

Zero Days are software vulnerabilities that are unknown to the software vendor or developer and have not been patched or fixed to date.
Heartbleed or Shellshock or Log4J.
Typically due the nature of zero days, organizations are left to rely on risk mitigation and avoidance strategies Implement things like compensating controls until an official patch from the vendor is released.

9. Supply Chain Attack :

Supply Chain Attack targets the software supply chain to compromise the security downstream to organizations or users. So instead of directly attacking a target organization, systems, or networks, attackers are going to exploit vulnerabilities or weaknesses in the software or services provided by third parties, vendors, or partners.

ABHINAV SHARMA

//ABHINAVSHA007

Ask How, When and Why?