**ATLAN CHALLENGE ROUND**

**Solution Document**

**Prepared By : Vijay Ganiger**

**PROBLEM 1 : Describe the process and approach of how a security operations team should handle security alerts.**

Security alerts help organizations quickly detect advanced cyber attacks.

It’s important that our security analysts are focused on the right security alerts. I Will try to explain with the help of examples.

**For Example 1** : **Privileged User & Account Monitoring**

**Solution ->** \*Privileged user accounts are one of the most common security weaknesses for organizations. End users with endpoints can have administrator or root privileges which can lead to downloading malicious software, making changes to network or system settings, or inadvertently letting a hacker obtain access to sensitive data.

**How to handle these above alert?**

* our security team should create dashboards to track privileged user activity. Hackers regularly attempt to obtain privileged user accounts and ways to escalate privileges as they are an entry to other systems and applications on your network.
* If a hacker has access to one of your privileged accounts, they can potentially bypass firewalls or Intrusion Detection Systems (IDS)

**For Example 2** : **Abnormal External Communication**

* our security team may be investigating lots of inbound traffic but, we need to check wheather they are monitoring abnormal outbound activity as well . External communication can take place on your network through an abnormal port or protocol.
* Your firewall can help with traffic filtering but may not catch everything. Abnormal external communication could be a hacker attempting to deploy malicious software, carry on Command and Control Activities.

**How to handle these above alert?**

* our security team should review how external communications are filtered, monitored, and blocked.External communications toward an open resource are typically allowed, but if the communication is not for public resources, then it could be an unauthorized communication.
* Any traffic that gives cause for concern should be validated against your security policy and reviewed against malicious patterns. Security alerts can be generated from your IDS/IPS, firewalls, and switches to monitor these external communications. And of course, the best way to monitor all of these is with a SIEM.

**For Example 3 : Data Exfiltration/Unusual Port Activity**

* Data exfiltration is one of the main objectives for advanced persistent threats (APTs). Threat actors can infiltrate frequently used ports to avoid firewalls and IDS and steal your company data. Or, they can use phishing and other social methods for infiltrating your environment.
* Commonly used ports for data exfiltration include common Internet services, hoping that they’ll have an any/any rule for that port on firewalls:

TCP: 80 (HTTP)

TCP: 443 (HTTPS)

TCP/UDP:53 (DNS)

Hackers typically use the following techniques to conduct an attack:

Backdoors: collects files and uses ports like 80, 443, and 53 to hide traffic

Web applications: an attacker can access data directly from web pages using ports above

* File transfer protocol (FTP): hackers use FTP as it’s a standard for transferring files – use SFTP or FTPS instead, or even better, use a secure cloud provider.

**How to handle this above alert ?**

* Our security team can set up alerts using your network intrusion and prevention system logs to identify any of the suspicious port activity mentioned above. our team may find that the traffic represents malware infiltration.
* our team could also consider setting up specific security alerts when data is shared externally more than normal. It could be a threat actor or insider stealing company data.
* Have a SIEM configuration that baselines what normal traffic looks like, and alerts when traffic outside the baseline occurs.

**Problem 2 : How can we protect our web applications and network from threats (e.g. OWASP top 10)?**

**Solution** -> I WILL TRY TO EXPLAIN WITH THE HELP OF VULNERABILITIES

1. **Broken authentication** :

* Multifactor authentication can help reduce the risk of compromised accounts, and automated static analysis is highly useful in finding such flaws,while manual static analysis can add strength when evaluating custom authentication schemes.
* Coverity SAST includes a checker that specifically identifies broken authentication vulnerabilities. Seeker IAST can detect hardcoded passwords and credentials, as well improper authentication or missing critical steps in authentication

1. **Server-Side Request Forgery :**

* Seeker is one of the modern AST tools that can track, monitor, and detect SSRF without the need for additional scanning and triaging. Due to its advanced instrumentation and agent-based technology, Seeker can pick up any potential exploits from SSRF as well.

1. **Software and Data Integrity Failures :**

* Application security tools help detect deserialization flaws, and penetration testing can validate the problem. seeker IAST can also check for unsafe deserialization and help detect insecure redirects or any tampering with token access algorithms.

1. **Security Misconfiguration :**

* Solutions like Coverity SAST include a checker that identifies the information exposure available through an error message. Dynamic tools like Seeker IAST can detect information disclosure and inappropriate HTTP header configurations during application runtime testing.

**Problem 3 : How do we prevent CIA from being compromised? Describe and give examples for each**

**Solution ->** There are many ways to ensure confindentiality

1. **Confindentiality :**

* Passwords, access control lists and authentication procedures use software to control access to resources. these access control methods are complemented by the use encryption to protect information that can be accessed despite the controls, such as emails that are in transit.
* Additional confidentiality countermeasures include administrative solutions such as policies and training, as well as physical controls that prevent people from accessing facilities and equipment.

1. **Integrity :**

* Access control and rigorous authentication can help prevent authorized users from making unauthorized changes.Hash verifications and digital signatures can help ensure that transactions are authentic and that files have not been modified or corrupted.
* Equally important to protecting data integrity are administrative controls such as separation of duties and training.

1. **Availability** :

* Systems that have a high requirement for continuous uptime should have significant hardware redundancy with backup servers and data storage immediately available. For large, enterprise systems it is common to have redundant systems in separate physical locations.
* Software tools should be in place to monitor system performance and network traffic. Countermeasures to protect against DoS attacks include firewalls and routers.

**Problem 4 : What are some basic security knowledge that every employee should have? How can we promote security awareness within the organisation?**

**Solution ->** Basic security knowledge that employee should have is regarding CIA triad

**Security awareness within organisaion :**

1. Nurture a healthy security culture

2. Provide security training for people

3. Implement a security strategy

4. Strengthen your IT security

5. Set a security goal

**Problem 5 : What security implementations can you recommend for each OSI layer?**

**Physical Layer :**

* Is used for defining the technical qualifications of the data connectivity. Since the security in this layer is critical, so in case of any cyber danger (DoS attack), it is recommended to unplug the cable from the primary system.Safeguarding this layer needs bio-metric security, camera-based surveillance, key cards, and other physical monitoring.

**Data** **Link Layer** :

* Comprises of data packets transported from the physical layer. Any malfunctioning in this layer or data breach can impede the working of the network layer.
* Vulnerabilities that can be used and attacks that can be made in this layer are MAC address spoofing and virtual-LAN circumvention.So for protecting your system, common security mechanisms are MAC address filtering, assessment of wireless applications, checking of proper data encryption standards.

**Network Layer :**

* is the last of the media layer and has an association with the real world. It deals with the addressing and routing of packets. IP address spoofing is one of the common attack of this phase.
* Strengthening this layer needs the techniques of firm anti-spoofing, proper implementation of firewalls and routing filters, and secure routing protocols.

**Transport Layer :**

* Comes under the logical layer, which helps in transferring variable-length data sequence. The reliability of this layer can be achieved by ensuring the segmentation and de-segmentation mechanism and error control.
* For security purposes, this layer needs an appropriate firewall, restrictive admission of transmission protocols, and appropriate port number.

**Session Layer** :

* Essentially manages the inter-system communication and sessions. The handling of local and remote application's interaction is done in this layer. In case of weak authentication methods, it can help attackers to perform a brute force.
* So the effective way of securing this layer is by ensuring appropriate encrypted key exchange, along with the restriction of unsuccessful session attempts using timing methods.

**Presentation Layer :**

* Is used to standardize data with the help of various conversion schemes. But if there is poor conduct of malicious input, it can help cybercriminals exploit the system or even crash a system.
* Separate sanitized input and proper input validation can help protect the system from attackers.

**Application Layer** :

* Contain the UI and the closest of all layers for the user-end. The widest range of cyber attacks and security breaches is possible in this layer.
* It can lead to shutting down the network, stealing data, crashing the application, manipulating the information sent from source to destination, and many more

**Problem 6** :

**Study the following case study. Share what you have learned from the case study and how the situation can be avoided in the future.**

**Solution ->**

**SINGHEALTH DATA BREACH : CASE STUDTY**

**Things I have learned from the case study:**

**->** Employees did not have adequate levels of cybersecurity awareness, training, and resources to appreciate the security implications of their findings and to respond effectively to the attack.

-> Employees holding key roles in IT security incident response and reporting failed to take appropriate, effective, or timely action, resulting in missed opportunities to prevent the stealing and ex-filtrating of data in the attack.

-> There were a number of vulnerabilities, weaknesses, and misconfigurations in network and system that contributed to the attacker’s success in obtaining and exfiltrating the data, many of which could have been remedied before the attack.

**Things to keep remember to avoid this kind of attacks in future :-**

**1.Predictable passwords are weak passwords ->**

**\*** one of the reasons why SingHealth was exposed to this insane data breach was due to weak password usage. One of SingHealth’s local administrator accounts functioned with the password, “P@ssword”… which is about as tough to crack as you can imagine.

\* Hackers are not only equipped with fast brains and faster fingers – they also have software to help them dig through predictable password variants. Start using tougher passwords.

**2. Crucial firmware and software updates can’t be missed**

\*We should never procrastinate for installation of windows updates and certain program and software on our PC .

\*SinghHealth folly came when local staff put off patching Microsoft Outlook, which could have defended them against a hacking tool used on an end-user workstation.

**3.There are big threats, and then there are bigger threats**

\*It’s important not to underestimate the severity of cyber attacks and malicious software out there. You might think you’re adequately protected, but there’s always something new that will dominate your defenses.

\*Technology is an ever-changing, ever-evolving force, and you can be sure that hacking capabilities grow as sure as your security measures improve as well.

**4. Hacking tools are widespread on the Internet**

\*And hackers out there are always in possession of arsenal in the form of advanced hacking tools and malicious software.It’s better to be vigilant than complacent, and this awareness needs to be passed on to your tech team and security experts.

\* Even frontline staff and non-tech employees should be educated on the dangers of cybersecurity weakness. It’s time to get your people to stop resting on their laurels and help them become more alert.

**5. Competent engineers and developers need to be onboard**

\*Coding vulnerabilities and weaknesses were detected in SingHealth’s security infrastructure as well, and that too led to the unfortunate data breach and hack earlier this year.

\* It falls to employers and technical leads to arm their organisations with competent and skilled engineers and developers. Without them, you leave your door wide open to malware and more. It’s time to start hiring smart and putting a tough team into place that’ll make any hacker’s life difficult.

**6. Network protection and security is paramount to any organisation**

\*One of the most important aspects of your digital infrastructure to protect is the organisational network. Once an open door is detected in your internal network, it might be difficult to flush out the hack or breach.

\* Weak networks are bad networks – SingHealth probably knows this best. Once a workstation was exploited and hacked into, it led to a domino effect that resulted in the exposure of millions’ personal data.