INCIDENCE RESPONSE PLAYBOOK

NETWORK SECURITY

1. **Triage**

- Review all existing network security tools, thresholds, policies, and processes.
- Review trending cybersecurity incidents and trends
- Access the organization's threat intelligence, and existing attack signatures against recent cyberattacks.
- Increase security awareness among employees through intensive training and education.
- Update the network architecture diagram and make them easily accessible to authorized users.

2. **Investigation**

- Implement monitoring systems to monitor the network traffic for any abnormal behavior.
- Employ intrusion detection systems to examine network traffic and detect malicious packets.
- Capture and preserve network packets and transactions for further analysis.
- Assign severity levels to each incident and determine the associated impact it can have.
- Set an investigation scope and analyze captured packets to determine the root cause of the incident.
- Engage the incident response team to trace the scope of the attack.

3. **Containment**

- Isolate all impacted network segments and hosts.
- block all unnecessary ports and services.
- Examine the network and efficiently patch identified vulnerabilities or resolve system misconfiguration.
- Update the network firewalls.

4. **Remediation**

- Update all outdated network devices.
- Remediate all impacted network systems.
- Restore all isolated network systems and monitor the activities of suspicious behaviors.
- Test all network security control to ensure that they function effectively and efficiently.
- Tighten network security controls.

WINDOWS SECURITY

1. **Triage**

- Review all existing windows security tools, policies, and processes.
- Classify all windows systems according to their level of criticality and importance.
- Review all windows endpoints and ensure that they are up-to-date.
- Increase security awareness among employees through intensive training and education.
- Devise an incident response plan and communicate it with all stakeholders.
- Ensure that all recovery systems are up-to-date and robust.
- Create system images of each system.

2. **Investigation**

- Implement monitoring systems to monitor system behaviors.
- Employ intrusion detection systems to analyze system activities and detect malicious packets.
- Log all events that take place on each system.
- Employ log analysis tools to evaluate the systems logs and determine how the incident occurred.
- Set proper analysis scope must be set to able to determine the root cause of the event and subsequent actions that the attacker performed on the system.
- Assign severity levels to each incident and evaluate the associated impact it can have.

3. **Containment**

- Disconnect affected systems from unaffected ones.
- Create a forensic image of each affected system for future investigations.
- Change system passwords to prevent unauthorized access or subsequent attacks

4. **Remediation**

- Tighten windows security controls
- Restore the compromised systems using the system images.
- Rebuild all impacted systems to clear the remnants of malicious software.
- Install windows security patches in a timely manner.
- Thoroughly test new security controls which have been implemented.
- Monitor the actions of suspicious behaviors to update the threat intel and signatures.

USER SECURITY

1. **Triage**

- Classify your resource and the users according to the level of importance and functionalities. Different resources and personnel require different levels of protection.
- Assess each user account to determine the level of impact an attack could have on the organization.
- Employ monitoring systems to monitor and detect any suspicious activity on any user account such as unauthorized but successful logins, excess failed login attempts within a given timeframe and unauthorized addition of new users, and escalation of privileges.
- Log all user activities on a system. Access to such log files should be restricted to only administrators.
- Devise an incident response plan and communicate it with all stakeholders.

2. **Investigation**

- Implement automated detection systems that will analyze and report any suspicious activity.
- Vulnerability assessment should be carried out on all systems associated with user accounts in question.
- Collect detailed log files on user accounts for further analysis.
- Define your investigation scope and analyze all activities logged on user accounts and systems that are captured within the scope.

3. **Containment**

- All systems associated with compromised accounts should be isolated from the network.
- Forensic system images should be captured and stored for further investigation.
- Compromised user accounts should be restricted or blocked from accessing the system.
- Change user account passwords.
- Investigate the root cause of the account compromise to determine the level of impact caused by the compromise.

4. **Remediation**

- Install security patches and change the passwords for all compromised accounts.
- Isolated systems can be reconnected.
- Restore secure system images and restore data from backups.
- Testing every unit of the restored system as well as the entire system to make sure that everything works perfectly.

References

Yee, L., & Aw, D (2021). Cyber Incident Response Playbook. Retrieved March 6, 2023 from https://www.ssa.org.sg/wp-content/uploads/2021/09/Cyber-Incident-Response-Playbook.pdf

CISA (2021). Federal Government Cybersecurity Incident & Vulnerability Response Playbooks. Cybersecurity and Infrastructure Security Agency