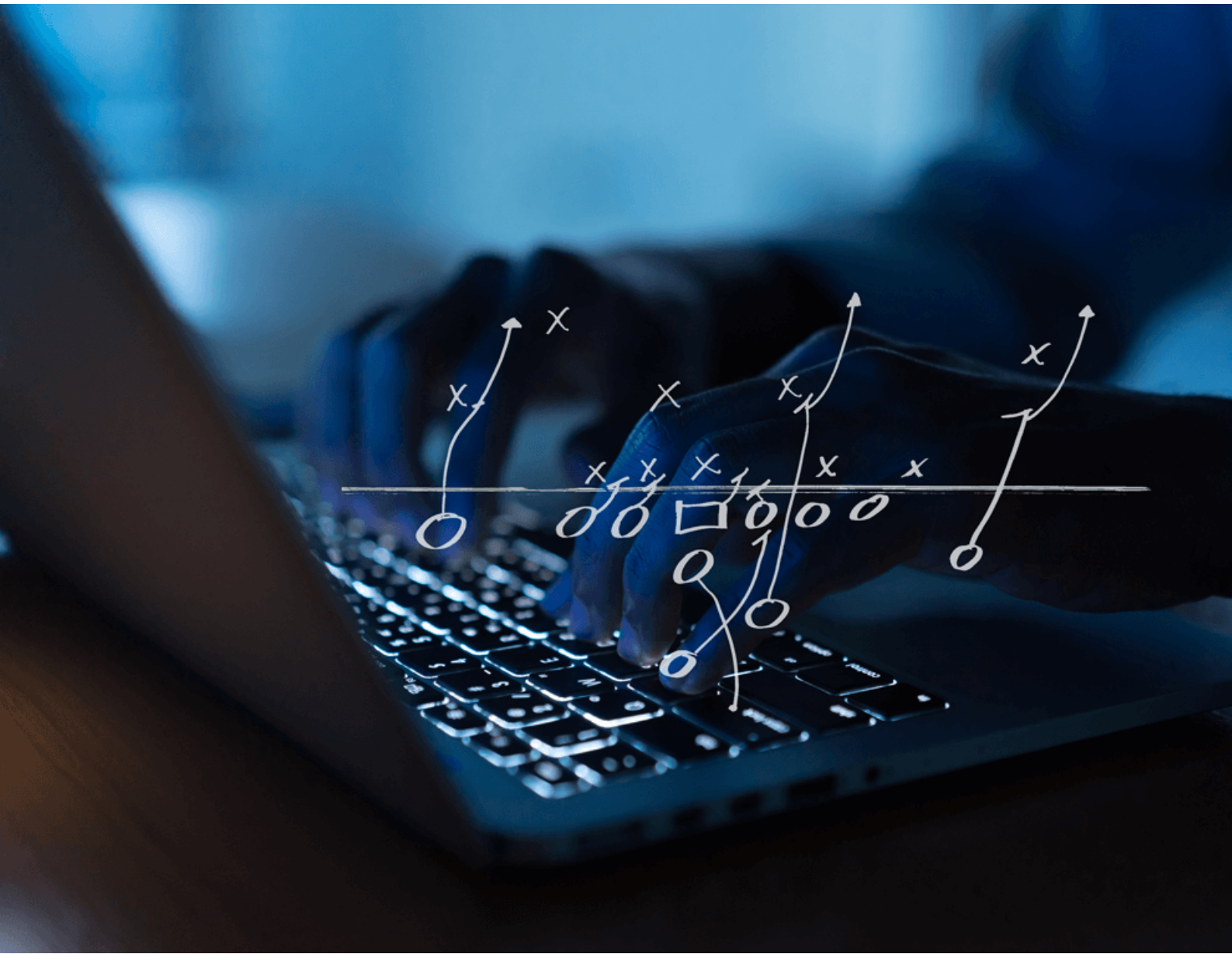
# INCIDENT RESPONSE PLAYBOOK

Created By:
Gopi Gor



# TABLE OF CONTENTS

# Executive Summary

An incident response playbook, tells us how to make sure the correct steps are taken in case an alert or potential threat has been raised in the system.

It does not focus on a specific threat but a more general reference for SOC analysts to use when any group of threats occur.

For this report, we will be focusing on 3 main types of alert or detection types related to sections within User Security, Network Security and Web Application Security. Each section will provide a method to triage, investigate, contain and remediate incase that type occurs.

**Objective:**

Create a general playbook for incident response, explaining that all attacks come under a specific type and general things should be done as first step.

# User Security

User security means protecting users, and endpoints from any kind of compromise like stealing of credentials. Examples could be account lockouts, unauthorized activity, keyloggers stealing passwords, etc.

**Triage:** For user security, to triage this alert , we need to first find the account which was compromised, and then we can check the severity of the stage along with all details of that account like if passwords were changed, which other users were contacted, etc.

**Investigation:** Investigation for a user based alert, can be done first by looking at all the logs including terminal logs which show if users have logged in remotely anywhere Following this we can also look if there are any anamoly in the user behaviours, random logins at multiple locations and finally check the system for any unusual downloads.

**Containment:** For a user account security activity, the first thing would be to isolate the account and do a complete backup and reset. Additionally, all passwords should be changed and multifactor authentication methods should be used in more extensive ways.

**Remediation:** For remediation, the user can be informed of the current scenarios and made aware about the situation, trained and how to avoid the mistake made in the initial stage by them. Furthermore, a forensic analysis can be conducted to understand the extent of the attack or threat and the ability of it to affect other host systems and the network.

# Web Application Security

Web Application Security means protecting any and all the websites or applications that are hosted on web servers, The types of web application security alerts that can be raised are SQL Injection, Cross-Site Scripting, Stealing of credentials, page not reachable errors or Server-Side Request Forgery.

**Triage:** First, analyze the logs and check all the access controls along with user credentials. The alert should be identified and shortlisted for which possible vulnerability was close to being exploited. The current applications, web server versions etc. should be collected before the investigation has started.

**Investigation:** First, we can run a penetration test to understand all the current vulnerabilties present in the web servers. Following this, the web code can be thoroughly reviewed to make sure that there are no errors that allow XSS or SQLi. If the web application uses any proxy or firewall, additional logs can be reviewed for this as well.

**Containment:** For containment of these kinds of alerts, the current system can be completed patched and upgraded, alongwith changes made in the configuration that improve the security. Contact the admininstrator of the web application to inform of a potential threat to the website, therefore altering it for the company too.

**Remediation:** The remediation can start by implementing Web Application Firewalls, and the user inputs can be validated. The security controls should be monitored regularly along with a hardening process.

# Network Security

Network Security means protecting the network and all the servers in the network and endpoints from any kind of changes, modifications, sniffing of packets and alteration to these packets. Few types of network security related alerts are network intrusions, malicious payloads being transferred, denial of service attacks, or abnormal connection requests and port numbers.

**Triage:** To triage the network security related alerts, we need to detect what kind of alert has occurred specifically to take the steps. After this the severity of that alert has to be defined with regards to the network parameters in the organization. Finally context information should be collected with regards to the network.

**Investigation:** To investigate this alert, we need to view the network traffic in detail by using a packet analyser like Wireshark and then look for changes in behaviour or weird port numbers. If there is an IDS or IPDS, these logs can be checked too. Finally, the network can be scanned for any vulnerabilities that may be existing in the network that can be exploited.

**Containment:** For containing these types, this could mean to isolate systems that may have malicious traffic included in it or completely block these malicious traffic and IP's from the network to avoid any further spreading in the network.

**Remediation:** For remediation, the ports that are open and not being currently used by any kinds of service can be completely closed until required. The firewalls can be used as next-gen firewalls, and the employees can be informed not to allow outside devices in the network  in any case.

# References


1. https://www.cybertriage.com/blog/training/how-to-investigate-user-logins-intro-to-incident-response-triage-2021/
2. https://www.cisco.com/site/us/en/learn/topics/security/what-is-user-security.html#jump-anchor-6
3. https://www.hostinger.com/tutorials/web-application-security?ppc_campaign=google_search_generic_hosting_all&bidkw=defaultkeyword&lo=9004077&gad_source=1&gclid=CjwKCAiA_5WvBhBAEiwAZtCU75gtbXM59wxOM1Jwr5n7g2TfsxBswRCwowzzUTeYZ1pjUzmF2oFb_RoCtHQQAvD_BwE#What_Is_Web_Application_Security
4. https://www.indusface.com/blog/application-security-how-prevention-beats-remediation/#:~:text=Remediation%20is%20a%20reactive%20approach,service%20disruptions%2C%20and%20so%20on.
5. https://www.eccouncil.org/cybersecurity-exchange/application-security/threat-mitigation-strategies-for-securing-web-applications/
6. https://www.ccslearningacademy.com/what-is-triage-in-cyber-security/#:~:text=Triage%20is%20a%20critical%20incident,resources%20can%20be%20allocated%20accordingly.
7. https://www.linkedin.com/pulse/process-investigating-alerts-cybersecurity-dorothy-mutahi/
8. https://flare.io/learn/resources/blog/cyber-risk-remediation-a-comprehensive-approach/#4-steps