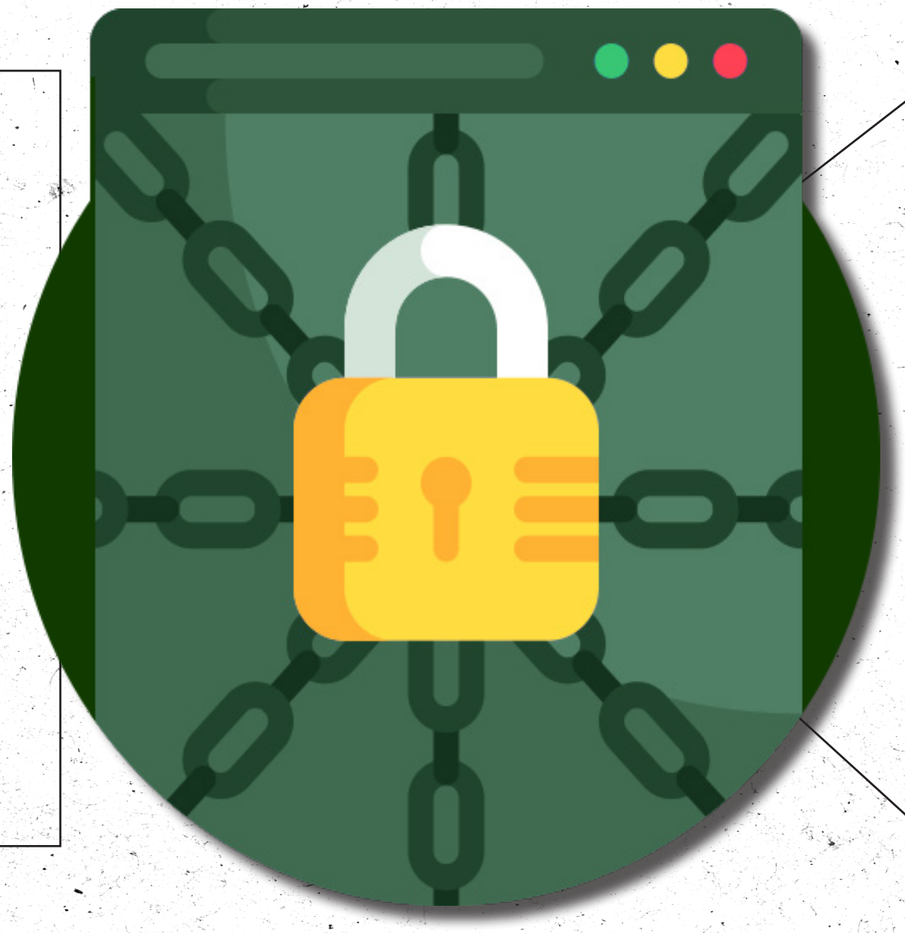
DAY 1/100

CYBER SPACE

RANSOMWARE

DETECTION TIME	ISOLATION TIME	RECOVERY TIME	CONTAINMENT SCOPE
< 10 MIN	< 10 MIN	< 10 MIN	< 10 MIN



DESCRIPTION

An endpoint or server exhibits signs of ransomware activity such as file encryption, ransom notes or alerts from EDR/XDR tools.

CATEGORY	DETAILS
INCIDENT TYPE	MALWARE - RANSOMWARE
SEVERITY	HIGH
PRIORITY	CRITICAL (DUE TO POTENTIAL BUSINESS IMPACT AND DATA LOSS)

PREPARATION :
Backup strategy, EDR with rollback, user awareness, logging (Windows, Sysmon, Network), ransomware IOC subscriptions

DETECTION & ANALYSIS :
Confirm ransomware activity, isolate host, identify strain, analyse logs and behaviour, MITRE ATT&CK mapping

CONTAINMENT :
Isolate affected systems, disable infected accounts, block external comms, snapshot impacted systems

ERADICATION :
Remove malware artifacts, patch vulnerabilities, perform full AV/EDR scan, validate removal

RECOVERY :
Restore from clean backup, rebuild if needed, monitor restored systems, reset passwords

LESSONS LEARNED :
Post-incident review, update detection rules, document findings, share IOCs

INSIDER THREAT

DETECTION TIME	INVESTIGATION TIME
< 10 MIN	< 1 HOUR

An internal employee, contractor or privileged user attempts to or successfully exfiltrates sensitive data through unauthorised channels such as personal email, cloud storage, removable media or file transfer tools.

CATEGORY	DETAILS
INCIDENT TYPE	INSIDER THREAT – DATA EXFILTRATION
SEVERITY	HIGH
PRIORITY	CRITICAL (DUE TO LEVEL OF DATA CONFIDENTIALITY)

PREPARATION :
Define sensitivity level on files, set policies, Log access, Educate employees, implement RBAC

DETECTION & ANALYSIS :
DLP violation, abnormal downloads with privilege escalation, Action intent, MITRE ATT&CK

CONTAINMENT :
block user access, block Exfiltration channels, Isolate Endpoint, Preserve Forensic Detail

ERADICATION :
Remove malware artifacts, enforce strict policies, correct misconfigurations

RECOVERY :
Restore from clean backup, Involve Legal Teams HR, Confirm data exfiltration

LESSONS LEARNED :
post incident analysis, strenghten monitoring, user training, report regulators, implement insider threat policy

CLOUD ACCOUNT COMPROMISED

DETECTION TIME	RESPONSE TIME	CONTAINMENT TIME	POST INCIDENT MONITORING
< 15 MIN	< 1 HOUR	<30 MIN	1-2 WEEKS

DESCRIPTION

An internal employee, contractor or privileged user attempts t An attacker gains unauthorized access to a user's cloud account, possibly through phishing, password spraying, token theft or OAuth abuse. The attacker may access email, storage, admin functions or cloud infrastructure. o or successfully exfiltrates sensitive data through unauthorised channels such as personal email, cloud storage, removable media or file transfer tools.

CATEGORY	DETAILS
INCIDENT TYPE	IDENTITY COMPROMISE – CLOUD ACCOUNT
SEVERITY	HIGH
PRIORITY	CRITICAL IF LATERAL MOVEMENT OR DATA ACCESS IS OBSERVED

PREPARATION :

Enable Logs and Monitor User Behavior, Implement MFA, Set Geo- Restrictions and login alerts , Apply Least Privilege

DETECTION & ANALYSIS :

Detect login anomalies like failed logins , impossible travel, MFA bypass . Correlate with Threat intel , Check MITRE map, Review access logs post compromise, check privilege escalation activities.

CONTAINMENT :

Revoke session and token , Reset Password, Suspend Account is impact is huge, Block Malicious IP Address

ERADICATION :

Remove malicious inbox rules or automations , disable rogue applications, review roles, restore modified data

RECOVERY :

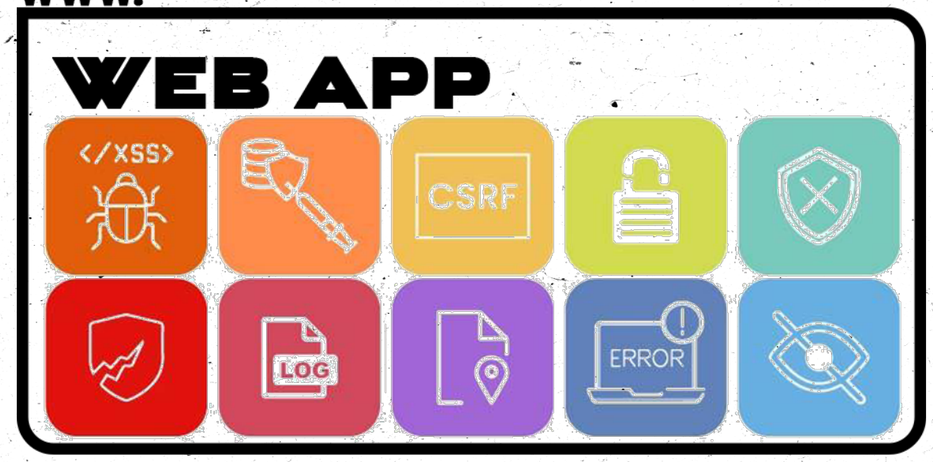
Re-enable account access, notify user and stakeholders, Monitor post recovery login anomalies, update existing access policies

LESSONS LEARNED :

Post Incident Analysis , Conduct RCA , Update Playbooks and detection rules, Educate Users, Fulfil legal reporting if any

EXPLOITATION WEB APP

WWW.



DETECTION TIME	PATCH TIME	CONTAINMENT TIME	POST INCIDENT RETEST
< 5 MIN	< 1 DAY	<30 MIN	< 2 DAYS

DESCRIPTION

An attacker exploits a vulnerability in a web application or server to gain unauthorised access, execute commands or extract sensitive data. The attack may be detected via WAF alerts, SIEM logs or anomalous behaviour.

CATEGORY	DETAILS
INCIDENT TYPE	APPLICATION-LAYER ATTACK
SEVERITY	HIGH
PRIORITY	HIGH

PREPARATION :

Conduct regular vulnerability assessments, implement a WAF, log HTTP Traffic , Patch , COde Review and DevSecOps Integration

DETECTION & ANALYSIS :

Alerts from WAF or SIEM , Review Logs, Validate input payloads in requests, Check for shelll uploads, privilege escalations, abnormal executions and MITRE ATT&CK mapping.

CONTAINMENT :

Block attacker IPs , Disable affected Web Apps, Isolate app server, Revoke session tokens

ERADICATION :

Remove malicious scripts or shells , Patched exploited vulnerabilities, Harden Architecture, Scan entire application stack

RECOVERY :

Restore services Monitor post- restoration , Notify affected users or customers, Conduct retest

LESSONS LEARNED :

Post Incident analysis, RCA, Update WAF and SIEM rules, improve secure coding practises, Report as required

USB MALWARE

DETECTION TIME	ISOLATION TIME	CONTAINMENT TIME	USB POLICY ENFORCEMENT
< 10 MIN	< 15 MIN	<30 MIN	100% REQUIRED

DESCRIPTION

Malicious software is introduced into the environment through an infected USB storage device. This may include autorun malware, ransomware, keyloggers or tools used to establish persistence or exfiltrate data.

CATEGORY	DETAILS
INCIDENT TYPE	PHYSICAL MEDIA-BASED MALWARE INFECTION
SEVERITY	MEDIUM TO HIGH
PRIORITY	HIGH

PREPARATION :

Disable USB autorun by Group policy settings, Implement USB control software, Enforce endpoint protection , Educate users and log USB usage

DETECTION & ANALYSIS :

Detect malware activity , Identify USB event and origin , Collect indicators, MITRE ATT&CK mapping

CONTAINMENT :

Isolate infected system , Remove USB Device and preserve for forensics, Block malicious Hash files, Identify other exposed systems

ERADICATION :

Remove malware, Delete suspicious files , Remove persistence mechanisms and perform full malware scan

RECOVERY :

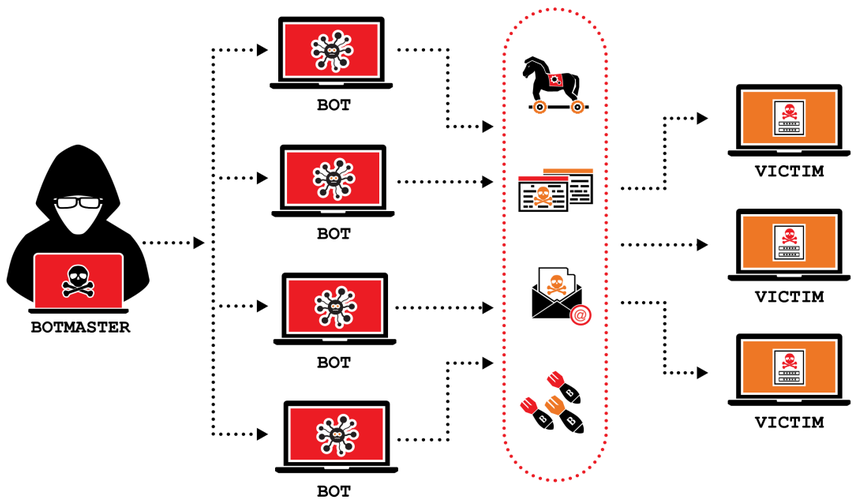
Restore system , Reinstate connectivity , Enable stricter USB policies liike allowing only for certain devices and Document the root cause

LESSONS LEARNED :

Post Incident analysis, RCA, Update USB policy

DDoS Attack

DETECTION TIME	MITIGATION TIME	SERVICE DOWNTIME	POST -MORTEM COMPLETION
< 5 MIN	< 15 MIN	<30 MIN	< 48 HOURS



DESCRIPTION

An external attacker launches a distributed denial-of-service (DDoS) attack targeting public-facing infrastructure such as websites, APIs, DNS servers or network gateways. The objective is to disrupt service availability, degrade performance or cause reputational and financial damage.

CATEGORY	DETAILS
INCIDENT TYPE	NETWORK/APPLICATION LAYER AVAILABILITY ATTACK
SEVERITY	HIGH
PRIORITY	CRITICAL - IF OUTAGE OCCURS

PREPARATION :

Implement DDoS protection , Deploy WAF and rate limiting , Ensure scable Infra, Establish communication with ISP , Conduct DDoS Drills

DETECTION & ANALYSIS :

Identify traffic surge , Determine attack vector, Correlate with logs, Confirm Impact, MITRE ATT&CK mapping

CONTAINMENT :

Engage cloud DDos Migration , Block malicious IPs, Implement rate limiting and filters, Redirect or reroute traffic

ERADICATION :

Drop Traffic from confirmed malicious sources, Adjust filtering rules, Remove temporary rules post attack , Investigate for blended threats

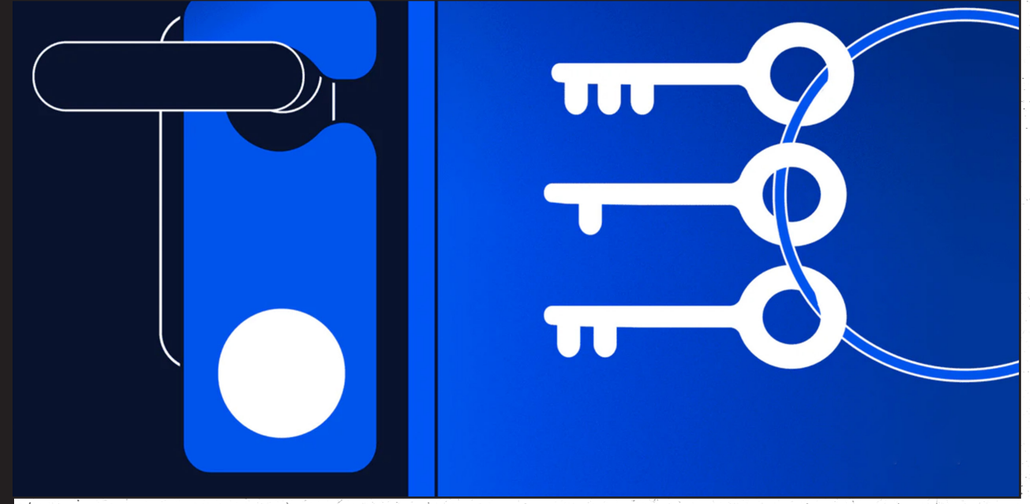
RECOVERY :

Monitor residual traffic , Confirm service restoration , Notify affected customers or partners , Resume Normal routing

LESSONS LEARNED :

Post Incident analysis, Mitigation effectiveness , Update response playbook , Report as required and improve vendor cordination

UNAUTHORISED PRIVILEGE ESCALATION



DETECTION TIME	RESTORATION TIME	CONTAINMENT TIME	REVIEW COMPLETION
< 5 MIN	< 1 HOUR	<30 MIN	< 48 HOURS

DESCRIPTION

An attacker, either through a vulnerability, misconfiguration or stolen credentials, escalates privileges from a low-privilege user to an administrative or root-level account, potentially compromising critical systems or accessing sensitive data.

CATEGORY	DETAILS
INCIDENT TYPE	ACCESS CONTROL VIOLATION / PRIVILEGE MISUSE
SEVERITY	HIGH TO CRITICAL
PRIORITY	HIGH

PREPARATION :

Implement RBAC , Least Privilege Principle, Monitor User Activity, Harden endpoints by patches, Enable Audit Logs

DETECTION & ANALYSIS :

Identify Alerts and correlate with user behavior, Analyse the process tree and validate persistence techniques along with MITRE ATT&CK mapping.

CONTAINMENT :

Disable affected user accounts and terminat all the elevated sessions and processes. Block the IPs, Notify IT or HR

ERADICATION :

Revert the permissions , Clean all persistence mechanisms like schedule tasks , registry modifications etc, Apply fixes for kernel-level or OS-level flaws

RECOVERY :

Re- enable original account , Restore system , operations and conduct post remidiation scan.

LESSONS LEARNED :

Document the escalation path, Update the SIEM detection rule, Improve Identity governance , report and Educate the privileged users.

CLOUD STORAGE MISCONFIG'N EXPOSURE

CATEGORY	DETAILS
INCIDENT TYPE	DATA EXPOSURE – MISCONFIGURATION
SEVERITY	HIGH TO CRITICAL
PRIORITY	HIGH

DETECTION TIME	MITIGATION TIME	EXPOSURE TIME	POLICY REMEDIATION TIME
< 1 HOUR	< 30 MIN	< 1 HOUR	< 72 HOURS

DESCRIPTION

Sensitive or confidential data (e.g., logs, databases, personal information) is exposed to the public due to misconfigured permissions on cloud storage services, often discovered via threat intelligence feeds, automated scanners or internal audits.

PREPARATION :

Enforce default secure policies , Implement CSPM tools, Enable access logging , Tag and classify sensitive adata, Perform regular cloud audits

DETECTION & ANALYSIS :

Review alert for CSPM on threat intel , Review object permissions , Access data sentivity, Check access logs and Map MITRE ATT&CK mapping

CONTAINMENT :

Restrict public access immediately and disable sharing links , Notify affected teams and Quarantine compromised credentials

ERADICATION :

Review and fix IAM policies , Enable bucket/ block level protection , Clean exposed data and reconfigure secure sharing mechanisms

RECOVERY :

Validate proper access controls , Confirm Data Integrity, Resume operations and update inventory

LESSONS LEARNED :

Document the escalation path, Conduct RCA, Update CSPM and SIEM detections, Train developers and DevOps Teams, Report if required and document the lessons learned.

UNAUTHORISED OAUTH APPLICATION SAAS

CATEGORY	DETAILS
INCIDENT TYPE	OAUTH ABUSE – UNAUTHORISED THIRD-PARTY APP
SEVERITY	HIGH
PRIORITY	HIGH TO CRITICAL

DETECTION TIME	MITIGATION TIME	SERVICE DOWNTIME	POST -MORTEM COMPLETION
< 5 MIN	< 15 MIN	<30 MIN	< 48 HOURS

DESCRIPTION

An employee or attacker grants a third-party application access to a corporate SaaS account using OAuth scopes (e.g., read email, access calendar, read/write files). These applications may exfiltrate data, impersonate users, or maintain persistent access without triggering standard credential or MFA alerts.

PREPARATION :

Restrict app consent policies, Monitor OAuth activity logs, Educate users, Integrate SSPM/CASP tools, Apply conditional access policies

DETECTION & ANALYSIS :

Alerts triggered, Identify user and application , Analyse access logs, Review app metadata, MITRE ATT&CK mapping

CONTAINMENT :

Revoke app access immediately , Suspend impacted user account, Block app domain or API end-point ,Notify user and security Team

ERADICATION :

Remove residual access token , Rotate credentials and MFA , Conduct full data access review, Update OAuth Policy

RECOVERY :

Reinstate user access with monitoring , Apply stricter app review process , Monitor for recurrence, validate SaaS logs and alerts.

LESSONS LEARNED :

Complete RCA , Improve user training , Strengthen OAuth governance , Document the incident , Notify affected parties or regulators.

ABUSE OF STOLEN SESSION TOKEN IN SAAS PLATFORM

CATEGORY	DETAILS
INCIDENT TYPE	ACCOUNT HIJACK – SESSION TOKEN ABUSE
SEVERITY	HIGH TO CRITICAL
PRIORITY	HIGH

SESSION REVOKE	ENDPOINT VALIDATION	MFA REIN-FORCEMENT	POST -MORTEM COMPLETION
< 10 MIN	< 1 HOUR	24 H	< 72 HOURS

DESCRIPTION

An attacker gains access to a valid session token (e.g., via XSS, phishing, malware or token theft from endpoints) and uses it to impersonate a legitimate user on a SaaS platform (e.g., Microsoft 365, Google Workspace, Salesforce, Slack). This allows access without triggering MFA or login anomaly alerts.

PREPARATION :

Enable session management logs , Deploy CASB and SaaS Security Tools, Use Conditional Access Policy , Educate users on phishing and token , Integrate endpoint protection

DETECTION & ANALYSIS :

Alerts triggered, Check for duplicate sessions , Review recent user activity , Analyse endpoint logs, MITRE ATT&CK mapping

CONTAINMENT :

Revoke all active sessions , Disable user account temporarily , Block attacker IP or devices, Notify user and support team

ERADICATION :

Scan endpoint for malware , Remove exposed credentials , Review session storage practises, Strenghten Saas Login Policies

RECOVERY :

Re- enable user access with strict monitoring , Monitor user activity closely, Educate user of session hijack , Internal drills needed

LESSONS LEARNED :

Complete RCA , Improve user training , Document the incident , Notify 3rd party or regulators

ZERO-DAY EXPLOITATION IN THIRD-PARTY LIBRARIES

DESCRIPTION

A critical vulnerability is disclosed (or actively exploited in the wild) in a third-party library or framework (e.g., Log4j, OpenSSL, Apache Struts, glibc) used within your environment. Attackers may exploit this zero-day before a patch or mitigation is available, often through remote code execution (RCE), information disclosure or privilege escalation.

CATEGORY	DETAILS
INCIDENT TYPE	ZERO-DAY EXPLOITATION – SUPPLY CHAIN / LIBRARY
SEVERITY	CRITICAL
PRIORITY	CRITICAL

PREPARATION :

Tag critical workloads using affected libraries, subscribe to TI & CVE feeds.

DETECTION & ANALYSIS :

Alerts triggered, Identify affected systems , Assess exposure , Monitor for IoCs , MITRE ATT&CK.

CONTAINMENT :

Isolate exposed services, Deploy WAF /IPS virtual patches, Remove or disable plugins / modules, Notify internal stakeholders.

ERADICATION :

Apply vendor patch or upgrade, Replace affected libraries, Remove Payloads and clean temporary mitigations.

RECOVERY :

Resume full operations , Conduct full forensics , Increase log temporarily , Verify 3rd party components

LESSONS LEARNED :

Document timeline , Update vulnerability management , Train Dev and Security Teams, Report Regulators , Conduct tabletop exercises post incident.

UNAUTHORIZED USE OF GENERATIVE AI TOOLS IN PRODUCTION

DETECTION TIME

< 10 MIN

CONTAINMENT TIME

< 30 MIN

< 24 HOURS

RISK ASSESSMENT

< 7 DAYS

COMPLIANCE REVIEW

DESCRIPTION

An employee or system uses a generative AI tool in a production environment - either by pasting sensitive code, data or configuration into an AI prompt or by integrating an AI assistant into a live application- without formal approval or proper security evaluation.

CATEGORY	DETAILS
INCIDENT TYPE	POLICY VIOLATION / DATA EXPOSURE RISK
SEVERITY	MEDIUM
PRIORITY	HIGH

PREPARATION :

Implement acceptable use policies , Monitor AI platform access, Use DLP and CASB , Enforce browser controls and blocking , Conduct user training.

DETECTION & ANALYSIS :

Detect unauthorized use, User or system , Review transmitted data, Usage context, MITRE ATT&CK mapping.

CONTAINMENT :

Block furthur access, Quarantine affected , Alert user and management , Capture forensic snap-shot.

ERADICATION :

Remove AI integration , Revoke any API tokens, exposed secrets , Clean up policy violation.

RECOVERY :

Restore access under policy , Validate codebase and production changes , Implement AI governance checks , Resume operations.

LESSONS LEARNED :

Conduct RCA , Update monitoring , Improce internal education , Document the incident and Report if required.

CONTINUOUS INTEGRATION / CONTINUOUS EXPLOITATION

CI/CD PIPELINE EXPLOITATION

DETECTION TIME
< 10 MIN

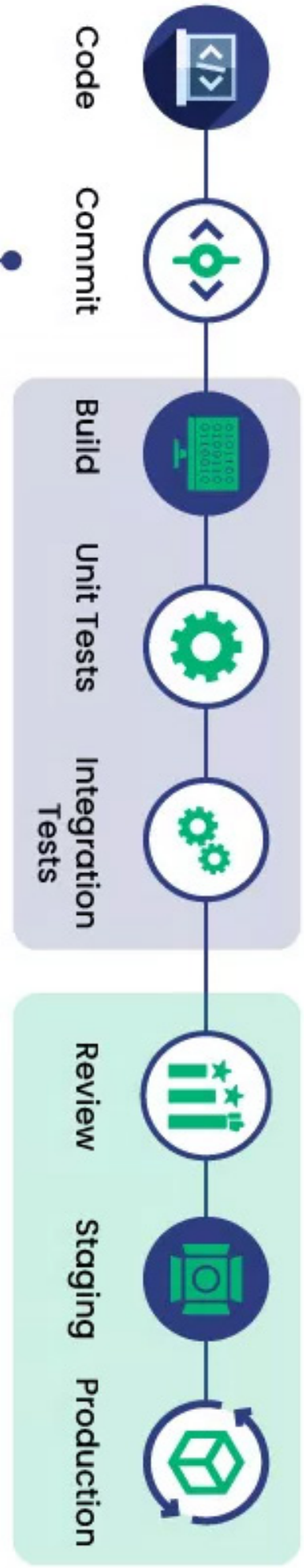
CONTAINMENT TIME
< 30 MIN

< 24 HOURS
RISK ASSESSMENT

< 7 DAYS
COMPLIANCE REVIEW

DESCRIPTION

An attacker gains access to or exploits weaknesses in a CI/CD pipeline (e.g., Jenkins, GitLab CI, GitHub Actions) to manipulate build processes, inject malicious code or secrets or use the pipeline to pivot into broader infrastructure.



CATEGORY	DETAILS
INCIDENT TYPE	SOFTWARE SUPPLY CHAIN / PIPELINE COMPROMISE
SEVERITY	HIGH TO CRITICAL
PRIORITY	CRITICAL

PREPARATION :

Enforce RBAC on CI/CD tools, Enable detailed audit logging , user signed commits and artifacts, Monitor pipeline abuse , Isolate build environments

DETECTION & ANALYSIS :

Alert from SIEM or DevSecOps , Review recent changes , Analyse source repoo , Identify affected projects, MITRE mapping

CONTAINMENT :

Disable affected pipelines , Revoke access to CI/CD tool , Block malicious artifacts , Isolate affected environments

ERADICATION :

Clean malicious code or scripts, Rotate compromised secrets , Patch vulnerabilities, Audit 3rd part integrations

RECOVERY :

Restore trusted pipelines , Rebuild affected apps , Re- enable deployments , Notify stakeholders

LESSONS LEARNED :

Conduct RCA , Update pipeline security , Train DevOps , Report and Update playbooks