Part 1 — Integrated Enterprise Threat Model

1.1 Assets Identification

Assets Identification	*Description*	Security Importance (CIA)	Asset Criticality	Associated Data
Cloud Web Applications	These applications serve as the organization's main external interface, enabling users to access online services, submit information, and interact with hosted functionalities.	C: Moderate–High I: High A: Very High	High	Session identifiers, customer activity logs, user-submitted content, and limited
Active Directory and Identity Systems	Core authentication infrastructure controlling account validation, authorization decisions, and policy distribution across internal systems.	C: Very High. I: Very High. A: Very High Asset	Critical	Credential hashes, authentication tokens, permission definitions, domain configurations.
CI/CD Pipeline Components	The system is responsible for generating, testing, and preparing software releases. It automates deployment flows and manages build artifacts.	C: High I: Critical. A: Medium–High	High	Source code repositories, script configurations, deployment secrets, compiled artifacts.

VPN and Remote Access Infrastructure	Provides authenticated employees with encrypted access to internal network segments from remote locations.	C: High. I: High. A: High	High	User authentication details, encrypted tunnels, metadata on connected devices.
R&D Data Stores	Dedicated storage for sensitive research outputs, technical documentation, and intellectual property belonging to ongoing development projects.	C: Extremely High. I: Very High. • A: High	Critical	Design drafts, experimental results, proprietary models, confidential strategic documents.
DNS / Network Infrastructure	Foundation for network communication, responsible for name resolution, routing paths, and service discoverability.	C: Medium. I: High. A: Very High	High	DNS zones, routing entries, load-balancing configurations, firewall rules.
On-Premises and Remote Endpoints	End-user and developer devices that interact with internal systems, perform administrative operations, and access sensitive resources.	C: High. I: High. A: Medium	Medium–High	Locally stored credentials, cached tokens, internal documents, development files.

1.2 Adversary Profiles

Category	State-Sponsored APT	Financially Motivated Cybercriminal	Insider with Internal Access
Motivation	Pursuing long-term intelligence objectives, obtaining strategic and highly sensitive	Financial gain via extortion, ransom, selling data, or disruption.	Financial gain, revenge, negligence.
Capabilities	Zero-day exploits, custom malware, stealth techniques, advanced lateral movement, and exploitation of AD and DNS.	Ransomware kits, botnets, password-guessing tools, ready-made malware.	Legitimate trusted access, knowledge of procedures, ability to bypass controls quietly.
Typical Targets	Active Directory, VPN systems, R&D repositories, CI/CD pipeline.	Public web apps, weak VPN accounts, endpoints, monetizable databases.	R&D repositories, internal documents, CI/CD pipeline, configuration files.
Typical Techniques	Spear-phishing, VPN compromise, identity manipulation, CI/CD tampering, covert C2 channels, DNS poisoning.	DDoS attacks, credential-stuffing, phishing, ransomware deployment, exploiting DNS misconfigurations.	Exfiltration, disabling logs, modifying permissions, uploading malicious files, misusing internal access.

Comparison:

- APTs → stealthy & long-term.
- Cybercriminals → fast disruption & extortion
- Insiders → abuse legitimate access

1.3 Attack Surface & Entry Points

- **Public Endpoints (Cloud Web Apps)**
  SQLi, XSS, authentication bypass, DDoS floods.

- **VPN Gateways**
  Credential stuffing, MFA bypass, VPN vulnerabilities.

- **Wi-Fi Networks**
  MITM, rogue APs, fake login pages, eavesdropping.

- **DNS Infrastructure**
  DNS poisoning, redirection to malicious servers.

- **Third-Party Dependencies**
  Supply-chain tampering, malicious updates.

- **Developer Endpoints**
  Phishing, malware, credential theft.

1.4 STRIDE + CIA Risk Analysis

1. Active Directory & Identity Systems

STRIDE Risks:

- Spoofing: Credential theft and forged Kerberos tickets.
- Tampering: Unauthorized changes to permissions or group policies.
- Repudiation: Weak auditing allows denial of malicious actions.
- Information Disclosure: Exposure of hashes and internal identity data.
- Denial of Service: Locking accounts or disabling controllers.
- Elevation of Privilege: Escalation to domain admin through misconfigurations.

CIA Priority:
C: Very High | I: Very High | A: Very High

Justification:
Confidentiality, integrity, and availability are all very high because AD controls authentication for the entire environment.

2. Cloud Web Applications

STRIDE Risks:
• Spoofing: Attacker impersonates legitimate users.
• Tampering: Modification of web data or API responses.
• Repudiation: Insufficient logs allow attackers to hide actions.
• Information Disclosure: Exposure of customer or session data.
• Denial of Service: DDoS attacks disrupting access.
• Elevation of Privilege: Bypassing access controls to gain admin roles.

CIA Priority:
C: Medium–High | I: High | A: Very High

Justification:
Availability is highest due to public-facing services; integrity and confidentiality follow.

---

3. CI/CD Pipeline Components

STRIDE Risks:
• Spoofing: Using stolen developer accounts.
• Tampering: Injecting malicious code or altering build artifacts.
• Repudiation: Hidden build changes without traceability.
• Information Disclosure: Leakage of source code or secrets.
• Denial of Service: Build failures stopping releases.
• Elevation of Privilege: Gaining deployment-level access.

CIA Priority:
C: High | I: Critical | A: Medium–High

Justification:
Integrity is critical because pipeline tampering affects the whole supply chain.

---

4. VPN & Remote Access Systems

STRIDE Risks:
• Spoofing: Stolen credentials allow unauthorized login.
• Tampering: Manipulating VPN configuration files.
• Repudiation: Insufficient session logs.
• Information Disclosure: Misconfigurations leaking session data.
• Denial of Service: Flooding or crashing VPN gateways.
• Elevation of Privilege: Compromising VPN admin accounts.

CIA Priority:
C: High | I: High | A: High

Justification:
Confidentiality and availability are highest because VPN carries internal traffic and must be accessible.

---

5. R&D Data Repositories

STRIDE Risks:
- Spoofing: Unauthorized access using compromised credentials.
- Tampering: Modifying or deleting research files.
- Repudiation: Untracked access to sensitive documents.
- Information Disclosure: Theft of proprietary R&D data.
- Denial of Service: Ransomware preventing access.
- Elevation of Privilege: Gaining access through incorrect ACLs.

CIA Priority:
C: Extremely High | I: Very High | A: High

Justification:
Confidentiality is the highest due to sensitive IP and research material.

---

6. DNS / Network Infrastructure

STRIDE Risks:
- Spoofing: Fake DNS responses.
- Tampering: Changing DNS records to redirect traffic.
- Repudiation: Unlogged network changes.
- Information Disclosure: Revealing internal hostnames.
- Denial of Service: DNS amplification attacks.
- Elevation of Privilege: Gaining control of network equipment.

CIA Priority:
C: Medium | I: High | A: Very High

Justification:
Availability is highest; DNS failure disrupts everything.

---

7. Endpoints (Developer & User Devices)

STRIDE Risks:
• Spoofing: Using a compromised device to impersonate a user.
• Tampering: Malware altering system files or tools.
• Repudiation: Weak logs allow denial of malicious activity.
• Information Disclosure: Theft of local credentials or tokens.
• Denial of Service: Ransomware disabling devices.
• Elevation of Privilege: Local privilege escalation exploits.

CIA Priority:
C: High | I: High | A: Medium

Justification:
Confidentiality and integrity are most important since endpoints can be entry points for attackers.

Part 2 — Unified Attack Tree

The link below contains the completed attack tree for this assignment.

https://app.xmind.com/share/3c79AYDR

Part 3 — Multi-Vector Attack Narrative

Phase 1 – Reconnaissance

The operation starts with standard open-source intel gathering. The attackers map the organization’s public domains, cloud-hosted applications, and VPN entry points. They review developer profiles on LinkedIn and GitHub, pick up hints about the tech stack from exposed error messages and headers, and eventually stumble on a CI/CD status page that was unintentionally left public.

Phase 2 - Initial Access (Phishing, Spoofing, MITM)

Next, they move to a tailored phishing campaign. Developers receive emails posing as internal DevOps notices about a required VPN client update. The link redirects to a cloned SSO login page hosted on attacker infrastructure, with selective DNS manipulation to make the domain look legitimate for targeted victims.

In parallel, at a tech conference, the group deploys a fake Wi-Fi access point using the company’s SSID. Developers who connect are transparently proxied to the same counterfeit VPN login page, allowing the attackers to capture valid credentials and session tokens.

Phase 3 — Execution (VPN Compromise)

Armed with stolen logins and inconsistent MFA enforcement the attackers sign in through the corporate VPN as if they were legitimate remote employees. They install a lightweight RAT on the compromised developer laptop to maintain command-and-control and avoid relying solely on stolen credentials.

Phase 4 — Lateral Movement (AD & Internal Networks)

Once inside, they begin enumerating Active Directory, identifying key assets: file servers, the build server, R&D repositories, and internal API layers. Using credentials harvested from the developer’s machine and Kerberoasting attacks, they eventually obtain a privileged service account tied to the CI/CD environment.

With that access, they pivot into the build server, browse internal artifact repositories, and map connections across the microservices ecosystem and R&D storage systems.

Phase 5 — Persistence (CI/CD Backdoor)

To secure long-term persistence, the attackers alter a CI/CD build template, injecting a small backdoor into a frequently deployed microservice. Each time the service runs in production, it quietly opens an encrypted outbound channel back to attacker infrastructure.

Because the artifacts come from the official pipeline and are properly signed, they pass through normal security controls without raising suspicion.

Phase 6 — Evasion (DDoS Distraction)

To mask their internal activity, the group triggers a coordinated DDoS attack against public-facing applications. The SOC and infrastructure teams shift their focus to mitigation, traffic filtering, and emergency routing, giving the attackers room to operate with fewer eyes on internal anomalies.

During the distraction, the attackers finish preparing collected R&D data on an internal file share under their control.

Phase 7 — Exfiltration (Covert C2)

Finally, the data is compressed, encrypted, and exfiltrated slowly through the compromised microservice using normal HTTPS traffic to attacker-owned cloud storage. Additional fragments are tunneled through DNS queries to blend in with routine network traffic.

The company remains functional, unaware that persistent backdoors now exist across both developer endpoints and production systems—and that the attackers have already taken a complete copy of sensitive R&D information.

Part 4 — Defensive Architecture & Mitigation Framework

This section outlines a concise defensive framework that enhances enterprise resilience through preventive, detection, response, and recovery controls.

4.1 Preventive Controls:

- **Network Segmentation**
  Limits attacker movement across internal systems, reducing APT lateral movement.

- **Multi-Factor Authentication (MFA)**
  Prevents unauthorized access even if credentials are spoofed or stolen.

- **Patch Management & System Hardening**
  Reduces exploitable vulnerabilities during initial compromise.

- **Firewall Filtering & DDoS Rate-Limiting**
  Mitigates DDoS floods and restricts malicious traffic volumes before reaching critical services.

4.2 Detection Controls:

- **Network Traffic Monitoring & Anomaly Detection**
  Identifies abnormal traffic linked to DDoS, spoofing, DNS manipulation, or MITM behavior.

- **Log Analysis & SIEM Correlation**
  Detects unusual authentication attempts, log flooding, and suspicious internal activity.

- **Wireless IDS / IDS-IPS Alerts**
  Detects rogue AP behavior, spoofing attempts, and signatures of MITM activity.

- **Endpoint Detection & Response (EDR)**
  Captures malicious processes and suspicious actions during APT stages.

4.3 Response Controls:

- **Isolation of Affected Hosts (Containment)**
  Stops MITM, spoofing, or lateral movement by removing compromised devices from the network.

- **DDoS Scrubbing Activation**
  Redirects traffic through scrubbing centers to filter malicious volumetric attacks.

- **Credential Reset & Session Revocation**
  Neutralizes stolen credentials or hijacked sessions used by the attacker.

- **Incident Reporting & Evidence Preservation**
  Supports forensic analysis and documentation across APT phases.

4.4 Recovery & Resilience Controls:

- **Restoring Systems from Verified Clean Backups**
  Ensures all manipulated configurations, backdoors, or DNS tampering are removed.
- **Rebuilding & Patching Affected Systems**
  Eliminates exploited vulnerabilities before returning systems to production.
- **Validation & Functionality Testing**
  Confirms systems operate correctly after removing spoofing or MITM artifacts.
- **Updating Security Policies & Lessons Learned**
  Improves defenses and procedures based on incident findings.