



AN INTEGRATED CYBERSECURITY AND GOVERNANCE PROGRAMME: RESEARCH IN DATA SECURITY, COMPLIANCE, AND LESSONS FROM THE EQUIFAX INCIDENT

Module: ACCA5034 - Data Security and Compliance

Student Name: Christian Prida

Student Number: 242771

August 12, 2026.

TASK 1: RESEARCH IN DATA SECURITY AND COMPLIANCE

1. INTRODUCTION TO TASK 1

What would be the rapid acceleration of enterprise digital transformation in the current era, cloud migration and distribution remote workforce models have fundamentally invalidated the traditional perimeter-based on a "castle and moat" architecture. This legacy approach assumed that all actors, endpoints, and internal network traffic originating within a physically defined corporate perimeter were inherently trusted, while all external traffic was unreliable. Network perimeters were protected by monolithic hardware firewalls, intrusion detection and prevention systems (IDS/IPS), and virtual private network hubs (VPNs).

However, modern enterprise environments no longer have a static physical perimeter. Critical applications and databases are distributed across multi-cloud environments, such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform, as well as Software-as-a-Service (SaaS) environments including Salesforce and Microsoft 365. Concurrently, employees require persistent, global access to enterprise assets from unmanaged, remote endpoints over public networks.

This structural shift exposes two critical vulnerabilities in perimeter-based defences:

First, the premise of **implicit internal trust** allows adversaries who breach the external boundary-via credential theft, social engineering, zero-day exploits, or unpatched edge appliances-to move laterally across flat internal networks without friction.

Second, the practice of **traffic hairpinning**-routing remote employee connection request through centralized corporate data centers for security inspection-creates massive latency bottlenecks, degrades user experience, and reduces operational efficiency.

To address these security and architectural limitations, modern cybersecurity strategies have transitioned to continuous, context-aware access control models. This research paper presents an in-depth critical evaluation of the **Zero Trust Architecture (ZTA)** and strategies for **Securing the Hybrid Workforce** using **Zero Trust Network Access (ZTNA)**, **Secure Access Service Edge (SASE)**, and **Data Loss Prevention (DLP)**. Additionally, it incorporates the **Governance of Artificial Intelligence (AI) and Machine Learning (ML) Systems**, critically evaluating how contemporary organizations operationalize these paradigms across four foundational security capabilities: **Anticipate, Protect, Detect, and Automatically Respond**.

2. THE ZERO TRUST ARCHITECTURE (ZTA): PRINCIPLES, EFFICACY, AND METRICS

- Theoretical Foundations and Core Principles

According to my research, Zero Trust is not a standalone software product, vendor device, or isolated tool; is a comprehensive strategic cybersecurity architecture based on the "Never Trust, Always Verify" principle Formalized by the National Institute of Standards and Technology in NIST Special Publication 800-207, Zero Trust eliminates implicit trust based on physical location, the IP subnet or domain membership.

According to NIST SP 800-207, a Zero Trust deployment relies on three central tenets:

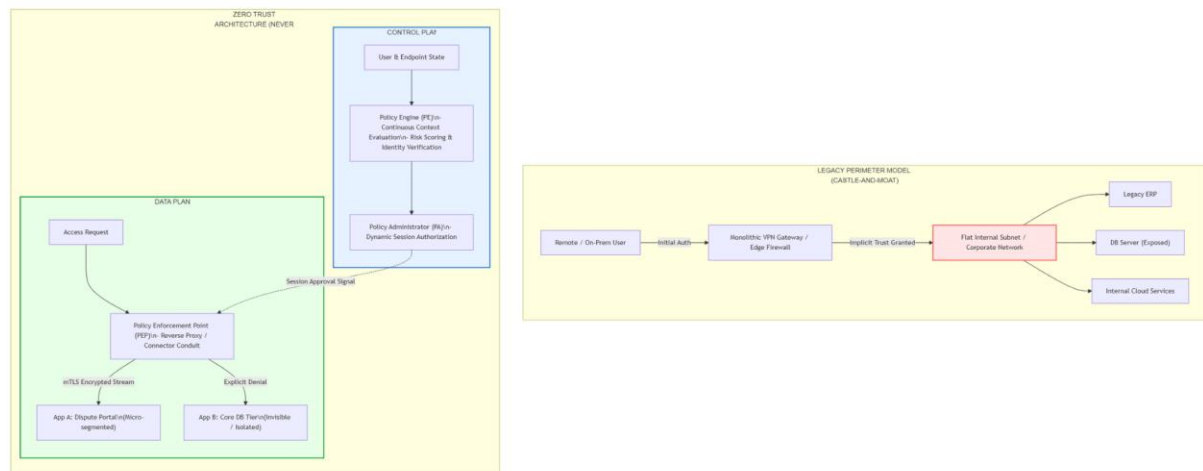
- A) **Explicit Verification:** Every access request-regardless of whether it originates from a senior executive inside corporate headquarters or an external automated service API-must be explicitly authenticated, authorized, and encrypted before access is granted. Evaluation decisions are calculated dynamically using real-time contextual indicators, including verified user identity, endpoint health posture, geographical location, target resource sensitivity, firmware integrity, and dynamic risk metrics.
 - B) **Least Privilege Access:** Access permissions are bounded using strict Just-In-Time (JIT) and Just-Enough-Access (JEA) frameworks. Contextual, risk-based access policies ensure users and workloads interact only with the specific application or data object required for an immediate task, eliminating broad network-level exposure.
 - C) **Assume Breach:** Security operations function under the explicit assumption that adversaries have already compromised internal network segments. Consequently, network environments are isolated into micro-segments, all traffic flows are encrypted end-to-end (both in transit and at rest), and continuous cross-domain telemetry is monitored to minimize attack blast radiuses.
- Comparative Efficacy: Perimeter-Based vs. Zero Trust Architectures

Under traditional perimeter models, access control is enforced once at the network edge via Layer 3 or Layer 4 firewalls and VPN entry points. Once authenticated, users receive broad IP-level access across entire subnets. This creates substantial exposure to lateral movement, credential abuse, and insider threats.

In contrast, Zero Trust Architectures decouple access control from physical network location, enforcing granular control at Layer 7 (Application Layer). Access decisions are processed through an explicit control plane divided into a Policy Engine (PE) and a Policy Administrator (PA), which govern execution points known as Policy Enforcement Points (PEPs). The Policy Engine continuously evaluates contextual risk signals against defined enterprise security policies. Once validated, the Policy

Administrator instructs the Policy Enforcement Point to establish an encrypted, application-specific session.

By shifting protection from physical subnets to individual applications, workloads, and data objects, Zero Trust Architectures eliminate implicit trust vectors. Lateral movement is neutralized because an adversary compromising a single application endpoint cannot discover or access adjacent internal network resources without passing explicit Policy Engine evaluations.



3. SECURITING THE HYBRID WORKFORCE: ZTNA, SASE, AND MODERN DLP

The expansion of remote work models has decentralized data storage across multi-cloud infrastructure and third-party SaaS ecosystems. Legacy Virtual Private Networks (VPNs) present major operational and security risks in these distributed environments:

- **Broad Network Access:** VPNs grant connected endpoints broad subnetwork visibility upon successful authentication. If a remote device is compromised by malware or credential theft, the entire internal network is exposed.
- **Routing Bottlenecks:** Directing all remote traffic through corporate data centers for centralized security filtering degrades network throughput and impairs cloud application performance.

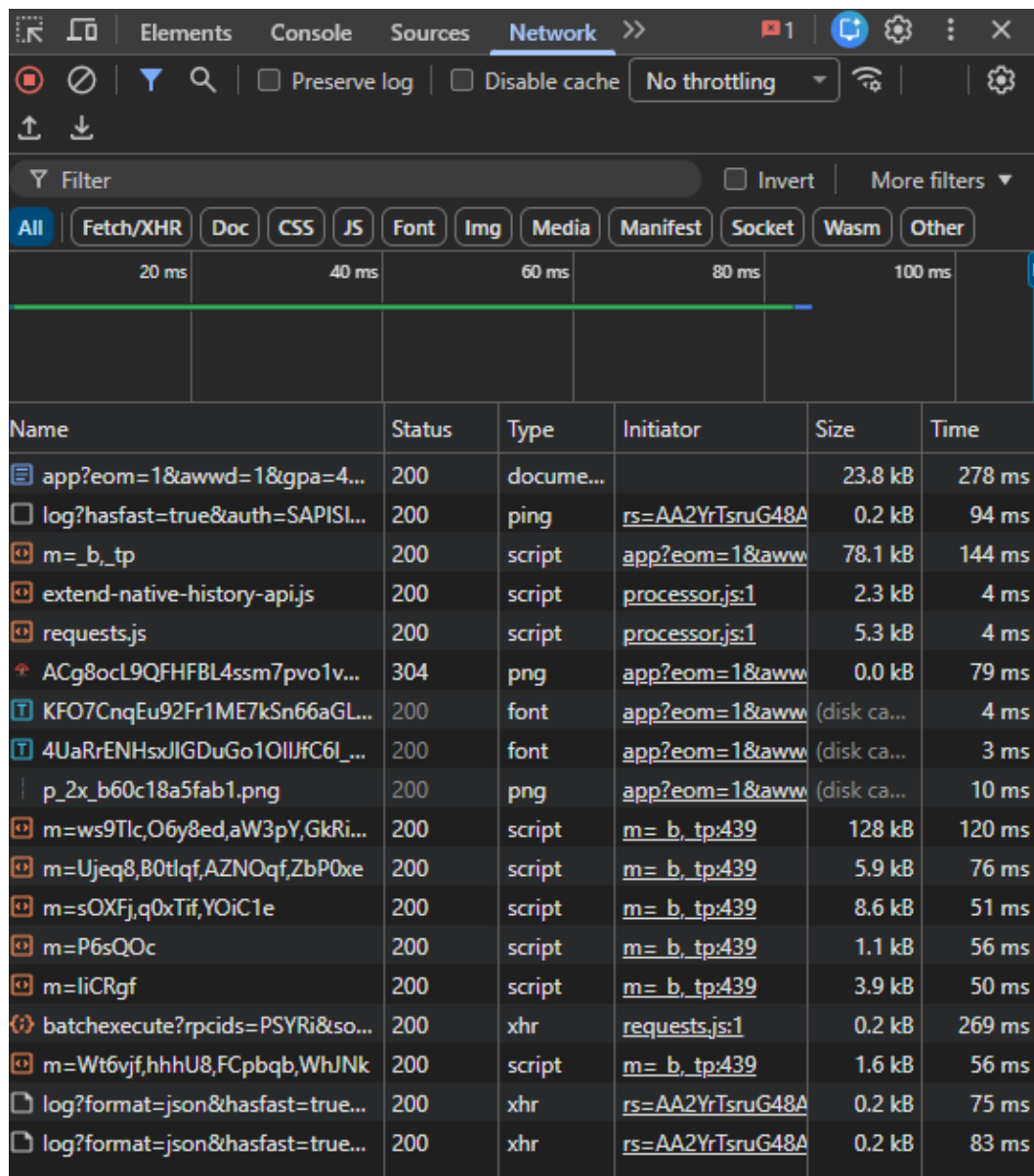
- Zero Trust Network Access (ZTNA)

Zero Trust Network Access establishes an identity-and context-aware boundary between users and individual applications. Operating on Software-Defined Perimeter (SDP) principles, ZTNA conceals private applications behind outbound-only connector conduits. As a result, internal application endpoints remain invisible to unauthorized users, eliminating external scanning and public port exposure.

- Secure Access Service Edge (SASE)

SASE converges Wide Area Networking (SD-WAN) with cloud-native security functions, known as Security Service Edge (SSE). Delivered through globally distributed cloud edge nodes, SASE enforces uniform security policies close to end-users without introducing routing latency. The SASE architecture integrates four core security capabilities:

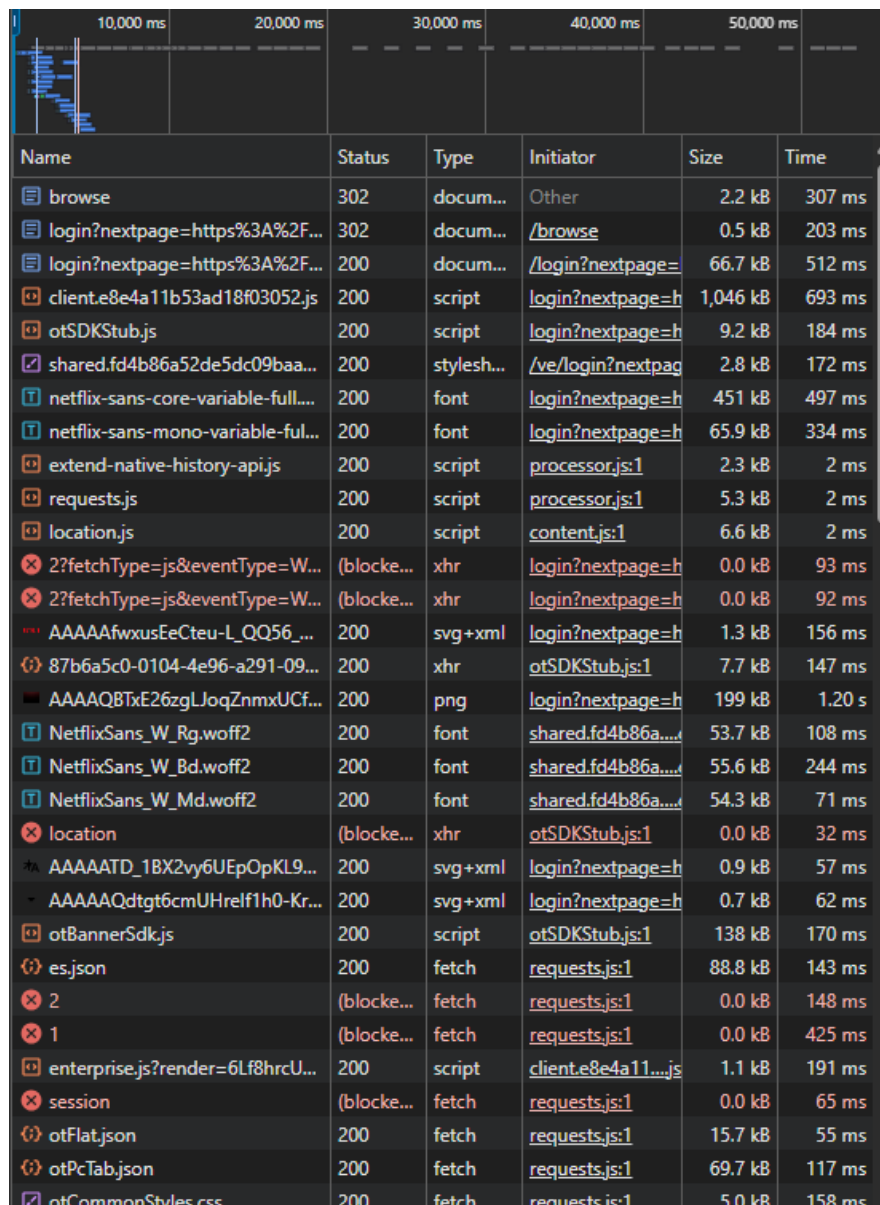
- 1) **Zero Trust Network Access (ZTNA)**: Delivers context-based access to private applications without opening broader network access.
- 2) **Secure Web Gateway (SWG)**: Filters malicious web traffic, executes URL classification, inspects encrypted session payloads, and prevents drive-by malware downloads.
- 3) **Cloud Access Security Broker (CASB)**: Enforces security policies between end-users and SaaS applications, providing visibility into unsanctioned shadow IT, monitoring API usage, and preventing unauthorized data sharing.
- 4) **Cloud-Native Data Loss Prevention (DLP)**: Inspects unstructured data in motion and at rest to enforce regulatory compliance across cloud environments.



Name	Status	Type	Initiator	Size	Time
app?eom=1&awwd=1&gpa=4...	200	docume...		23.8 kB	278 ms
log?hasfast=true&auth=SAPISL...	200	ping	rs=AA2YrTsrG48A	0.2 kB	94 ms
m=_b,_tp	200	script	app?eom=1&aww	78.1 kB	144 ms
extend-native-history-api.js	200	script	processor.js:1	2.3 kB	4 ms
requests.js	200	script	processor.js:1	5.3 kB	4 ms
ACg8ocL9QFHFBL4ssm7pvo1v...	304	png	app?eom=1&aww	0.0 kB	79 ms
KFO7CnqEu92Fr1ME7kSn66aGL...	200	font	app?eom=1&aww	(disk ca...	4 ms
4UaRrENHsxJIGDuGo1OIJfC6l_...	200	font	app?eom=1&aww	(disk ca...	3 ms
p_2x_b60c18a5fab1.png	200	png	app?eom=1&aww	(disk ca...	10 ms
m=ws9Tlc,O6y8ed,aW3pY,GkRi...	200	script	m= b, tp:439	128 kB	120 ms
m=Ujeq8,B0tlqf,AZNOqf,ZbP0xe	200	script	m= b, tp:439	5.9 kB	76 ms
m=sOXFj,q0xTif,YOiC1e	200	script	m= b, tp:439	8.6 kB	51 ms
m=P6sQOc	200	script	m= b, tp:439	1.1 kB	56 ms
m=liCRgf	200	script	m= b, tp:439	3.9 kB	50 ms
batchexecute?rpcids=PSYRi&so...	200	xhr	requests.js:1	0.2 kB	269 ms
m=Wt6vjf,hhhU8,FCpbqb,WhJNk	200	script	m= b, tp:439	1.6 kB	56 ms
log?format=json&hasfast=true...	200	xhr	rs=AA2YrTsrG48A	0.2 kB	75 ms
log?format=json&hasfast=true...	200	xhr	rs=AA2YrTsrG48A	0.2 kB	83 ms

- Next-Generation Data Loss Prevention (DLP)

Modern DLP solutions expand beyond legacy pattern-matching rules (such as basic regular expressions for social security or credit card numbers). By leveraging machine learning models, Optical Character Recognition (OCR) for scanned documentation, and Exact Data Marching (EDM) linked to database records, modern DLP monitors endpoints, cloud applications, and network streams in real time. It automatically blocks, quarantines, or encrypts sensitive assets-such as customer personal data, source code, and API credentials-before unauthorized exfiltration can occur.



Name	Status	Type	Initiator	Size	Time
browse	302	docum...	Other	2.2 kB	307 ms
login?nextpage=https%3A%2F...	302	docum...	/browse	0.5 kB	203 ms
login?nextpage=https%3A%2F...	200	docum...	/login?nextpage=	66.7 kB	512 ms
client.e8e4a11b53ad18f03052.js	200	script	login?nextpage=h	1,046 kB	693 ms
otSDKStub.js	200	script	login?nextpage=h	9.2 kB	184 ms
shared.fd4b86a52de5dc09baa...	200	stylesh...	/ve/login?nextpag	2.8 kB	172 ms
netflix-sans-core-variable-full...	200	font	login?nextpage=h	451 kB	497 ms
netflix-sans-mono-variable-ful...	200	font	login?nextpage=h	65.9 kB	334 ms
extend-native-history-api.js	200	script	processor.js:1	2.3 kB	2 ms
requests.js	200	script	processor.js:1	5.3 kB	2 ms
location.js	200	script	content.js:1	6.6 kB	2 ms
2?fetchType=js&eventType=W...	(blocke...	xhr	login?nextpage=h	0.0 kB	93 ms
2?fetchType=js&eventType=W...	(blocke...	xhr	login?nextpage=h	0.0 kB	92 ms
AAAAAfwxusEeCteu-L_QQ56_...	200	svg+xml	login?nextpage=h	1.3 kB	156 ms
87b6a5c0-0104-4e96-a291-09...	200	xhr	otSDKStub.js:1	7.7 kB	147 ms
AAAAAQBTxE26zgJJoqZnmXUCf...	200	png	login?nextpage=h	199 kB	1.20 s
NetflixSans_W_Rg.woff2	200	font	shared.fd4b86a....	53.7 kB	108 ms
NetflixSans_W_Bd.woff2	200	font	shared.fd4b86a....	55.6 kB	244 ms
NetflixSans_W_Md.woff2	200	font	shared.fd4b86a....	54.3 kB	71 ms
location	(blocke...	xhr	otSDKStub.js:1	0.0 kB	32 ms
AAAAATD_1BX2vy6UEpOpKL9...	200	svg+xml	login?nextpage=h	0.9 kB	57 ms
AAAAAQdtgt6cmUHrelf1h0-Kr...	200	svg+xml	login?nextpage=h	0.7 kB	62 ms
otBannerSdk.js	200	script	otSDKStub.js:1	138 kB	170 ms
es.json	200	fetch	requests.js:1	88.8 kB	143 ms
2	(blocke...	fetch	requests.js:1	0.0 kB	148 ms
1	(blocke...	fetch	requests.js:1	0.0 kB	425 ms
enterprise.js?render=6Lf8hrcU...	200	script	client.e8e4a11....js	1.1 kB	191 ms
session	(blocke...	fetch	requests.js:1	0.0 kB	65 ms
otFlat.json	200	fetch	requests.js:1	15.7 kB	55 ms
otPcTab.json	200	fetch	requests.js:1	69.7 kB	117 ms
otCommonStyles.css	200	fetch	requests.js:1	5.0 kB	158 ms

4. GOVERNANCE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING SYSTEMS

As organizations integrate Artificial Intelligence (AI) and Machine Learning (ML) models into business processes and automated security operations, establishing structured governance over AI data and models has become a critical requirement. AI and ML technologies introduce novel attack vectors that standard cybersecurity controls are not designed to mitigate.

- Key AI/ML Threat Vectors
 - i. **Data Poisoning Attacks:** Adversaries insert corrupted or biased samples into model training datasets, compromising

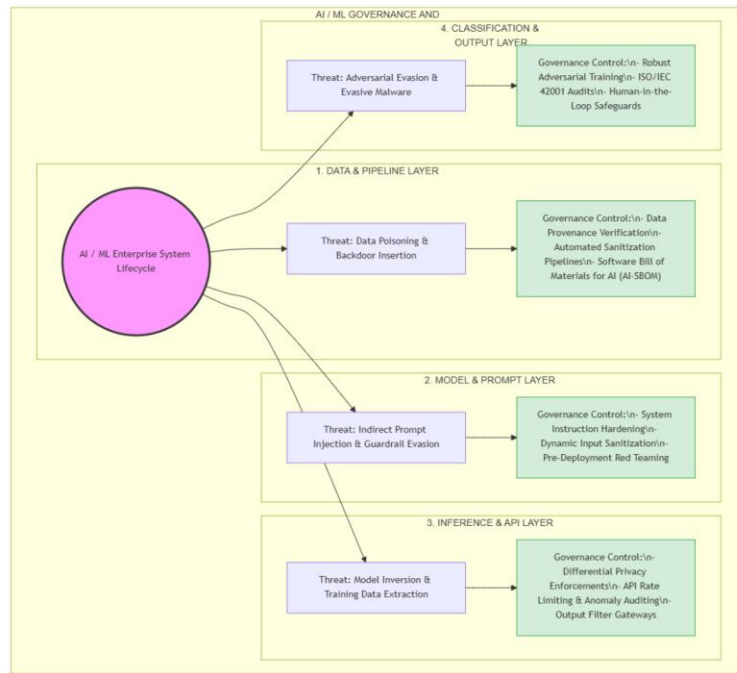
system logic, degrading predictive accuracy, or installing hidden backdoors.

- ii. **Prompt Injection and Data Exfiltration:** In Large Language Models (LLMs), malicious prompt injection bypasses system instruction guardrails, inducing the model to disclose confidential training data, execute unauthorized system commands, or override access limits.
- iii. **Model Inversion and Membership Inference:** Attackers issue queries to public model APIs and analyze output probabilities to reconstruct proprietary model algorithms or extract sensitive data used during training.
- iv. **Adversarial Evasion:** Inputs are subtly altered to manipulate machine learning classifiers, allowing malicious payloads-such as obfuscated malware-to be misclassified as benign files.

- Governance Frameworks and Responsible AI Practices

To manage AI-related risks, organizations align operations with recognized governance frameworks, including the **NIST AI Risk Management Framework (AI RMF 1.0)** and the **ISO/IEC 42001** standard for AI management systems.

- **Model Inventory and Lineage Tracking:** Maintaining a comprehensive asset inventory of all deployed AI models, training pipelines, and data sources, supported by a Software Bill of Materials for AI (AI-SBOM).
- **Data Provenance and Sanitization:** Enforcing strict data sanitization pipelines to strip sensitive personal data before model training or fine-tuning occurs.
- **AI Security Testing (Ted Teaming):** Conducting routine adversarial red-teaming techniques, and logic manipulation.
- **Regulatory Alignment:** Adhering to emerging legal requirements, such as the EU AI Act, ensuring high-risk AI deployments maintain human oversight, auditability, operational transparency, and rigorous technical security safeguards.



5. THE 4-PILLAR FUNCTIONAL CAPABILITY EVALUATION

To defend against advanced persistent threats (APTs) and automated exploitation toolkits, modern cybersecurity programs must operationalize four core capabilities:

- Anticipate

Anticipation focuses on identifying and reducing the enterprise attack surface before adversaries exploit vulnerabilities.

 - **External Attack Surface Management (EASM):** Continuously scans public IP ranges, subdomains, external API endpoints, and cloud assets to identify unmapped exposure points.
 - **Cloud Security Posture Management (CSPM):** Automatically audits multi-cloud configurations against security benchmarks (such as the CIS Controls) to remediate misconfigurations, clouding open storage buckets or overly permissive access policies.
 - **Threat Intelligence Integration:** Ingests real-time Indicator of Compromise (IOC) feeds into SIEM and XDR systems, mapping threat actor tactics against the MITRE ATT&CK framework.
- Protect

Protection mechanisms enforce access boundaries and secure sensitive assets against unauthorized manipulation.

 - **Phishing-Resistant Multi-factor Authentication (FIDO2-WebAuthn):** Replaces password-based and legacy SMS/TOTP codes with hardware-backend cryptographic credentials, neutralizing credential interception risks.

- **Micro-segmentation:** Divides networks into isolated logical segments governed by strict application-layer policies, preventing unrestricted lateral movement.
- **Data Encryption:** Enforces TLS 1.3 for data in transit and AES-256 for data at rest across endpoints, cloud databases, and backup repositories.

○ Detect

Detection capabilities monitor enterprise environments to identify anomalous behaviour, security breachers, and policy violations in real time.

- **Extended Detection and Response (XDR):** Aggregates cross-domain telemetry from endpoints, identity management systems, network appliances, and cloud workloads to expose complex attack sequences.
- **User and Entity Behaviour Analytics (UEBA):** Applies machine learning baselines to identify anomalous account actions, such as impossible geographic travel, rapid privilege escalation, or unusual database queries.

○ Automatically Respond

Automated response capabilities reduce threat dwell time by replacing manual incident response workflows with programmatic execution.

- **Security Orchestration, Automation, and Response (SOAR):** Executes pre-configured response playbooks immediately upon threat confirmation.
- **Automated Containment Actions:** Automatically revokes compromised user authentication tokens, enforces step-up authentication, disables compromised user directory accounts. And isolates infected endpoints from the network within seconds of detection.

```
Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> netstat -ano

Active Connections

Proto Local Address           Foreign Address         State       PID
TCP 0.0.0.0:135              0.0.0.0:0               LISTENING   1336
TCP 0.0.0.0:445              0.0.0.0:0               LISTENING   4
TCP 0.0.0.0:7680             0.0.0.0:0               LISTENING   4308
TCP 0.0.0.0:49174           0.0.0.0:0               LISTENING   1288
TCP 0.0.0.0:49664           0.0.0.0:0               LISTENING   944
TCP 0.0.0.0:49665           0.0.0.0:0               LISTENING   948
TCP 0.0.0.0:49666           0.0.0.0:0               LISTENING   1832
TCP 0.0.0.0:49667           0.0.0.0:0               LISTENING   1576
TCP 0.0.0.0:49669           0.0.0.0:0               LISTENING   8
TCP 0.0.0.0:51525          0.0.0.0:0               LISTENING   9296
TCP 0.0.0.0:57621          0.0.0.0:0               LISTENING   1288
TCP 127.0.0.1:6463          0.0.0.0:0               LISTENING   4296
TCP 127.0.0.1:7768          0.0.0.0:0               LISTENING   1288
TCP 127.0.0.1:8884          0.0.0.0:0               LISTENING   4
TCP 127.0.0.1:27060        0.0.0.0:0               LISTENING   7664
TCP 127.0.0.1:49682        0.0.0.0:0               LISTENING   7664
TCP 127.0.0.1:49682        127.0.0.1:49688         ESTABLISHED 7664
TCP 127.0.0.1:49684        0.0.0.0:0               LISTENING   7664
TCP 127.0.0.1:49684        127.0.0.1:49687         ESTABLISHED 7664
TCP 127.0.0.1:49687        127.0.0.1:49684         ESTABLISHED 8136
TCP 127.0.0.1:49688        127.0.0.1:49682         ESTABLISHED 8136
TCP 172.16.0.23:139        0.0.0.0:0               LISTENING   4
TCP 172.16.0.23:49901      3.233.158.20:443        ESTABLISHED 11748
TCP 172.16.0.23:50977      35.186.224.38:443       ESTABLISHED 1288
TCP 172.16.0.23:51247      52.110.1.100:443        ESTABLISHED 9120
TCP 172.16.0.23:51524      162.159.136.234:443     ESTABLISHED 10072
TCP 172.16.0.23:51918      20.50.201.206:443       ESTABLISHED 9120
TCP 172.16.0.23:53602      13.69.239.69:443        ESTABLISHED 9120
TCP 172.16.0.23:54033      13.73.244.6:8883        ESTABLISHED 2868
TCP 172.16.0.23:54052      172.217.113.4:443       TIME_WAIT   0
TCP 172.16.0.23:54391      104.16.102.112:443      ESTABLISHED 11748
TCP 172.16.0.23:54968      172.253.147.188:5228    ESTABLISHED 11748
TCP 172.16.0.23:55116      104.16.103.112:443      ESTABLISHED 11748
TCP 172.16.0.23:55340      23.103.225.65:443       ESTABLISHED 9120
TCP 172.16.0.23:55351      35.186.224.38:443       ESTABLISHED 6364
TCP 172.16.0.23:55705      192.178.50.67:443       ESTABLISHED 11748
TCP 172.16.0.23:56150      20.50.201.206:443       ESTABLISHED 9120
TCP 172.16.0.23:56419      192.178.50.67:443       ESTABLISHED 11748
TCP 172.16.0.23:56367      23.103.225.65:443       ESTABLISHED 9120
TCP 172.16.0.23:56859      40.126.28.20:443        ESTABLISHED 9120
TCP 172.16.0.23:57546      52.108.9.12:443         ESTABLISHED 9120
TCP 172.16.0.23:57874      52.110.2.141:443        ESTABLISHED 9120
TCP 172.16.0.23:58423      192.178.50.67:443       ESTABLISHED 11748
TCP 172.16.0.23:58928      23.219.3.217:443        ESTABLISHED 11748
TCP 172.16.0.23:59482      52.111.251.24:443       TIME_WAIT   0
TCP 172.16.0.23:59717      20.190.152.19:443       ESTABLISHED 9120
TCP 172.16.0.23:59765      52.123.251.43:443       ESTABLISHED 9120
TCP 172.16.0.23:59846      52.110.2.175:443        ESTABLISHED 9120
TCP 172.16.0.23:60435      104.16.102.112:443      TIME_WAIT   0
TCP 172.16.0.23:61467      23.221.66.131:443       ESTABLISHED 10072
TCP 172.16.0.23:61843      172.217.116.4:443       ESTABLISHED 11748
TCP 172.16.0.23:61928      35.186.224.39:443       ESTABLISHED 10072
TCP 172.16.0.23:63167      34.158.255.62:4070      ESTABLISHED 1288
```

6. IMPLEMENTATION CHALLENGES OF ZERO TRUST ARCHITECTURES

Despite its technical advantages, transitioning from legacy perimeter models to a Zero Trust Architecture involves notable operational challenges

1. **Legacy Infrastructure and Technical Debt:** Mainframes, legacy client-server software, and industrial control systems (OT) often lack support for modern identity protocols (such as SAML 2.0, OIDC, or FIDO2), requiring proxy-based integration workarounds.
2. **Policy Management Complexity:** Defining and maintaining micro-segmentation rules and context-aware policies across multi-cloud environments can lead to misconfigurations that disrupt operational workflows.
3. **User Friction and Change Management:** Intrusive step-up authentication prompts or overly restrictive DLP rules can hinder employee productivity, potentially driving the use of unapproved shadow IT solutions.
4. **Upfront Capital and Operational Investment:** Transitioning to unified SASE and ZTNA models requires dedicated financial investment, specialized engineering expertise, and ongoing operational oversight.

7. SUMMARY OF TASK 1

Transitioning from perimeter defenses to a Zero Trust Architecture is necessary to secure modern hybrid workforces and multi-cloud environments. By combining ZTNA, SASE, and cloud-native DLP with rigorous AI/ML governance, organizations establish identify-based boundaries that protect sensitive data assets across all environments. Operationalizing the Anticipate, Protect, Detect, and Auto-Respond framework ensures security teams can proactively mitigate risks, prevent lateral movement, and isolate threats in real time.

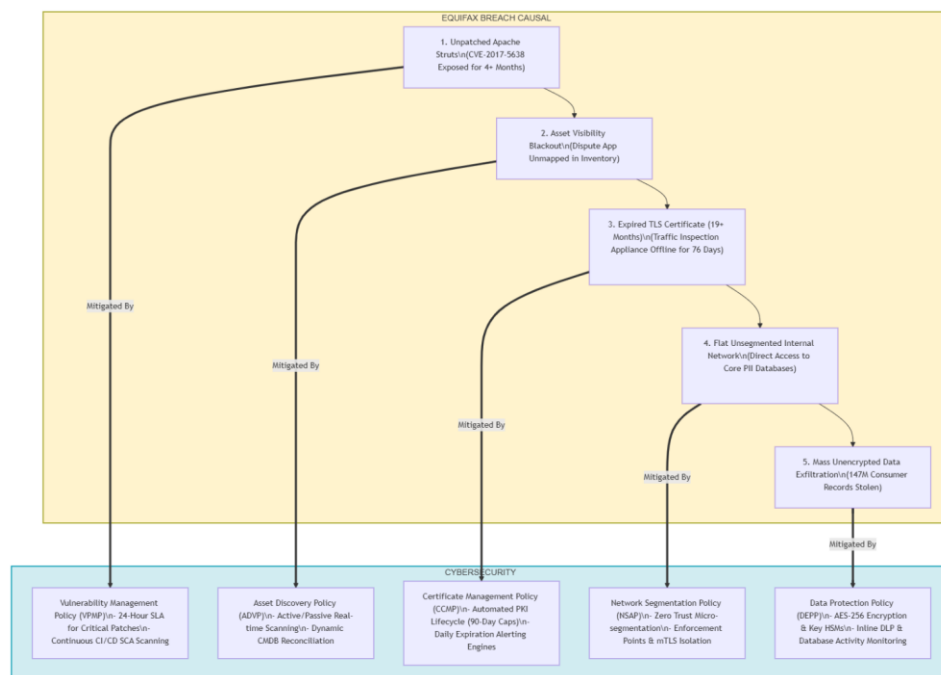
TASK 2: CASE SCENARIO & CYBERSECURITY PROGRAMME DESIGN (EQUIFAX LESSONS LEARNED)

1. INTRODUCTION AND EQUIFAX BREACH CONTEXT

In September 2017, Equifax disclosed one of the most consequential cybersecurity breaches in history, affecting approximately 157 million consumers. Attackers exfiltrated massive volumes of highly sensitive Personally Identifiable Information (PII), including Social Security numbers, dates of birth, full names, addresses, and driver's license details.

- **Structural Failures Exposing the Enterprise**
The breach occurred due to a series of operational, technical, and governance breakdowns:
 - **Vulnerability Management Failure:** US-CERT issued a critical alert regarding a remote code execution vulnerability in Apache Struts (CVE-2027-5638). Equifax failed to apply the available security patch to its online dispute portal for over four months.
 - **Asset Visibility Deficits:** IT operations and security teams lacked a unified, automated asset inventory, leaving the vulnerable dispute application unmonitored and unpatched.
 - **Inspection Blackout:** Attackers exfiltrated data undetected for 76 days because an internal network traffic inspection appliance was offline due to an expired digital certificate that had remained unrenewed for over 19 months.
 - **Flat Architecture and Unrestricted Access:** The dispute application was directly connected to unsegmented internal databases containing non-encrypted consumer PII.
 - **Governance Silos:** The Chief Information Security Officer (CISO) reported through the legal department rather than directly to executive leadership or the Board of Directors, delaying risk escalation and strategic decision-making.

The following sections present a structured cybersecurity programme designed to prevent these systemic vulnerabilities.



2. COMPONENT 1: ORGANISATIONAL STRUCTURE AND ACCOUNTABILITY

To address the governance failures observed in the Equifax incident, this cybersecurity programme establishes an independent organizational structure with clear reporting channels, executive oversight, and Board visibility.

- Leadership Roles and Operational Responsibilities

Board of Directors (Technology and Risk Committee)

- **Responsibility:** Maintains fiduciary oversight of enterprise cyber risk, approves cybersecurity capital budgets, and reviews quarterly risk metrics, including vulnerability remediation rates and Incident Response metrics.
- **Justification:** Ensures cybersecurity in management as a strategic enterprise risk rather than an isolated IT operational task.

Chief Executive Officer (CEO)

- **Responsibility:** Holds ultimate executive accountability for enterprise operational resilience and security posture alignment with corporate objectives.
- **Justification:** Centralizes executive decision-making across IT operations, risk governance, and business units.

Chief Information Security Officer (CISO)

- **Responsibility:** Directs enterprise cybersecurity strategy, vulnerability management, security architecture, and regulatory compliance. Reports directly to the CEO and provides quarterly briefings to the Board's Technology and Risk Committee.
- **Justification:** Separating the CISO from IT operations and legal departments avoids operational conflicts of interest, ensuring security priorities are not compromised for short-term operational speed or legal risk containment.

VP of DevSecOps and Application Security

- **Responsibility:** Implements automated security scanning (SAST, DAST, SCA) in development pipelines and maintains Software Bill of Materials (SBOM) tracking.
- **Justification:** Directly mitigates software vulnerabilities by integrating security testing into every stage of the software development lifecycle.

VP of Security Operations and Identify

- **Responsibility:** Manages the 24/7 Security Operations Center (SOC), Threat Intelligence feeds, Incident Response procedures, and Identity and Access Management (IAM).
- **Justification:** Unifies real-time monitoring, incident response, and access management under single operational leadership.

Director of Cyber Compliance and Risk

- **Responsibility:** Directs regulatory compliance (GDPR, DORA, NIS2), oversees independent security audits, and manages vendor supply chain risk assessments.
- **Justification:** Aligns technical controls with global statutory mandates and audit requirements.

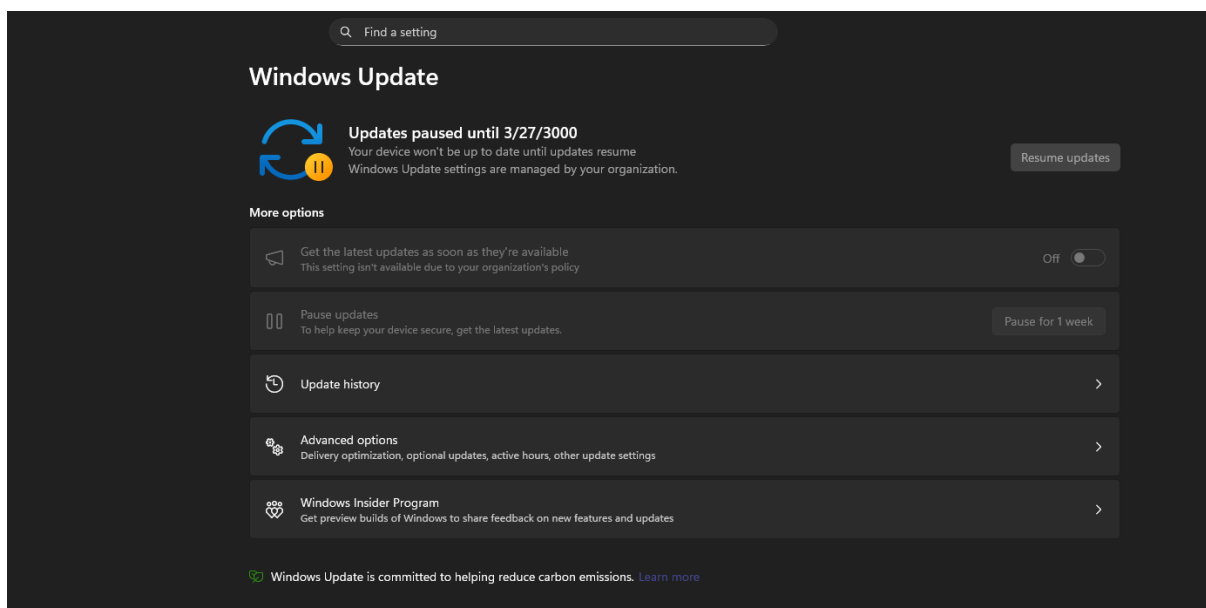
3. COMPONENT 2: POLICIES AND PROCEDURES

To remediate operational deficits in patch execution, asset tracking, and certificate monitoring, the enterprise enforces six mandatory policies.

- Policy Directives, Target Metrics, and Enforcement Mechanisms

Vulnerability and Patch Management Policy (VPMP)

- **Mandate:** All production environments, web frameworks, and application dependencies must undergo continuous scanning. Vulnerabilities must be remediated based on Common Vulnerability Scoring System (CVSS) severity tiers:
 - **Critical (CVSS 9.0-10.0):** Patch applied within 24 hours of public release or vendor notification.
 - **High (CVSS 7.0-8.9):** Patch applied within 7 days.
 - **Medium (CVSS 4.0-6.9):** Patch applied within 30 days.
- **Auditability:** Weekly automated compliance reports from scanning engines are cross-referenced with production deployment logs. Unremediated vulnerabilities automatically escalate to executive management.



Asset Discovery and Visibility Policy (ADVP)

- **Mandate:** Unregistered hardware, software, containers, or cloud assets are blocked from connecting to enterprise networks or cloud infrastructure. Active and passive discovery engines maintain a real-time inventory of all digital assets.
- **Auditability:** Monthly reconciliation audits compare Configuration Management Database (CMDB) records against active network traffic logs and cloud environment APIs.

Secure Software Development Lifecycle (S-SDLC) Policy

- **Mandate:** CI/CD deployment pipelines must integrate automated Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and Software Composition Analysis (SCA). Builds containing unresolved Critical or High vulnerabilities are automatically

blocked from production release. Every release requires a certified Software Bill of Materials (SBOM).

- **Auditability:** CI/CD logs require cryptographic attestation verifying that all automated security gates passed before deployment to production.

Certificate and Cryptographic Lifecycle Management Policy (CCMP)

- **Mandate:** All SSL/TLS digital certificates are managed through an automated Public Key Infrastructure (PKI) management platform. Maximum certificate validity is capped at 90 days, with automated renewal execution at 30 days prior to expiration.
- **Auditability:** Daily automated scanning monitors all internal and external endpoints for expiring, misconfigured, or invalid digital certificates, flagging discrepancies to the SOC.

Network Segmentation and Access Policy (NSAP)

- **Mandate:** Direct connectivity between internet-facing presentation layers and core database servers is strictly prohibited. Production application tiers communicate across micro-segmented boundaries governed by least-privilege firewalls and mutual TLS (mTLS) authentication.
- **Auditability:** Quarterly automated audits inspect network rule sets and cloud security groups to eliminate stale or permissive access rules.

Data Encryption and Protection Policy (DEPP)

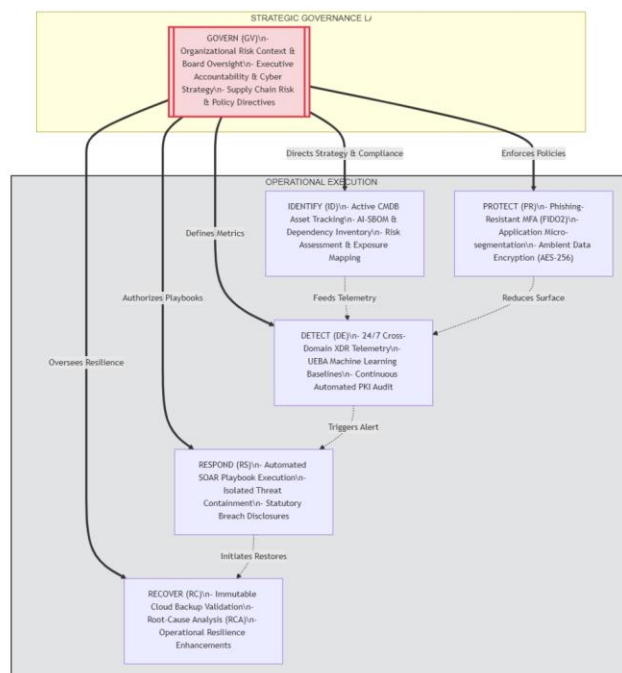
- **Mandate:** Sensitive customer information and PII must be encrypted both at rest (AES-256) and in transit (TLS 1.3). Encryption keys are stored in dedicated Hardware Security Modules (HSMs) separate from application data stores, with mandatory annual key rotation.
- **Auditability:** Real-time Database Activity Monitoring (DAM) logs and alerts on unencrypted queries or anomalous data retrieval attempts.

4. COMPONENT 3: GOVERNANCE AND STRATEGIC ALIGNMENT (NIST CSF 2.0)

To align cybersecurity execution with organizational objectives, the program implements the **NIST Cybersecurity Framework (CSF) 2.0**. The inclusion of the **GOVERN (GV)** function in version 2.0 ensures that governance, risk tolerance, and enterprise communication directly inform technical operations.

- NIST CSF 2.0 Strategic Implementation

- **GOVERN (GV):** Establishes organizational risk context, security policies, executive accountability, and supply chain risk strategies. Aligns cybersecurity spending with enterprise operational resilience goals.
- **IDENTIFY (ID):** Maintains comprehensive asset inventories, identifies software dependencies via SBOMs, conducts business impact analyses, and maps external exposure vectors
- **PROTECT (PR)** Enforces identity management via phishing-resistant MFA, applies micro-segmentation, enforces ambient data encryption, and executes automated patch deployments.
- **DETECT (DE):** Deploys 24/7 XDR, SIEM log correlation UEBA behavioral profiling, and continuous PKI monitoring to detect anomalous activity across endpoints and networks.
- **RESPOND (RS):** Executes automated SOAR playbooks, coordinates crisis communication channels, handles regulatory notifications and isolates affected infrastructure during security incidents.
- **RECOVER (RC):** Executes business continuity plans, validates immutable cloud backups, conducts post-incident root-cause analyses, and updates operational playbooks based on lessons learned.



5. COMPONENT 4: RISK MANAGEMENT AND ASSESSMENT

A structured risk assessment was conducted to quantify and prioritize systemic vulnerabilities similar to those exploited in the Equifax breach

- Risk Scoring Framework

Risk levels are evaluated using a 5x5 Likelihood(L) vs. Impact (I) matrix:

- Likelihood Scale: 1 (Rare), 2 (Unlikely), 3 (Possible), 4 (Likely), 5 (Almost Certain).
- Impact Scale: 1 (Insignificant), 2 (Minor), 3 (Moderate), 4 (Major), 5 (Catastrophic).
- Risk Classifications: Low (1-5), Medium (6-11), High (12-19), Critical (20-25).

- Quantitative Risk Assessment Matrix

Risk ID	Risk Scenario / Threat Vector	Inherent L	Inherent I	Inherent Risk	Mitigation Strategy	Residual Risk
R-01	Unpatched Web Framework: Exploitation of known remote code execution flaws (e.g., Apache Struts) on public web portals	5	5	25 (Critical)	Deploy CI/CD Software Composition Analysis, automated virtual patching via WAF, and enforce 24-hour SLA for Critical patches.	5 (Low)
R-02	Expired PKI Certificate: Inspection appliances miss exfiltration due to expired TLS decryption certificates.	4	5	20 (Critical)	Implement automated PKI certificate lifecycle management with auto-renewal and daily.	4 (Low)
R-03	Flat Internal Network: Attackers move laterally from presentation applications to backend database servers.	4	5	20 (Critical)	Enforce Zero Trust micro-segmentation, mTLS authentication, and isolate database subnets behind PEP gateways.	4 (Low)

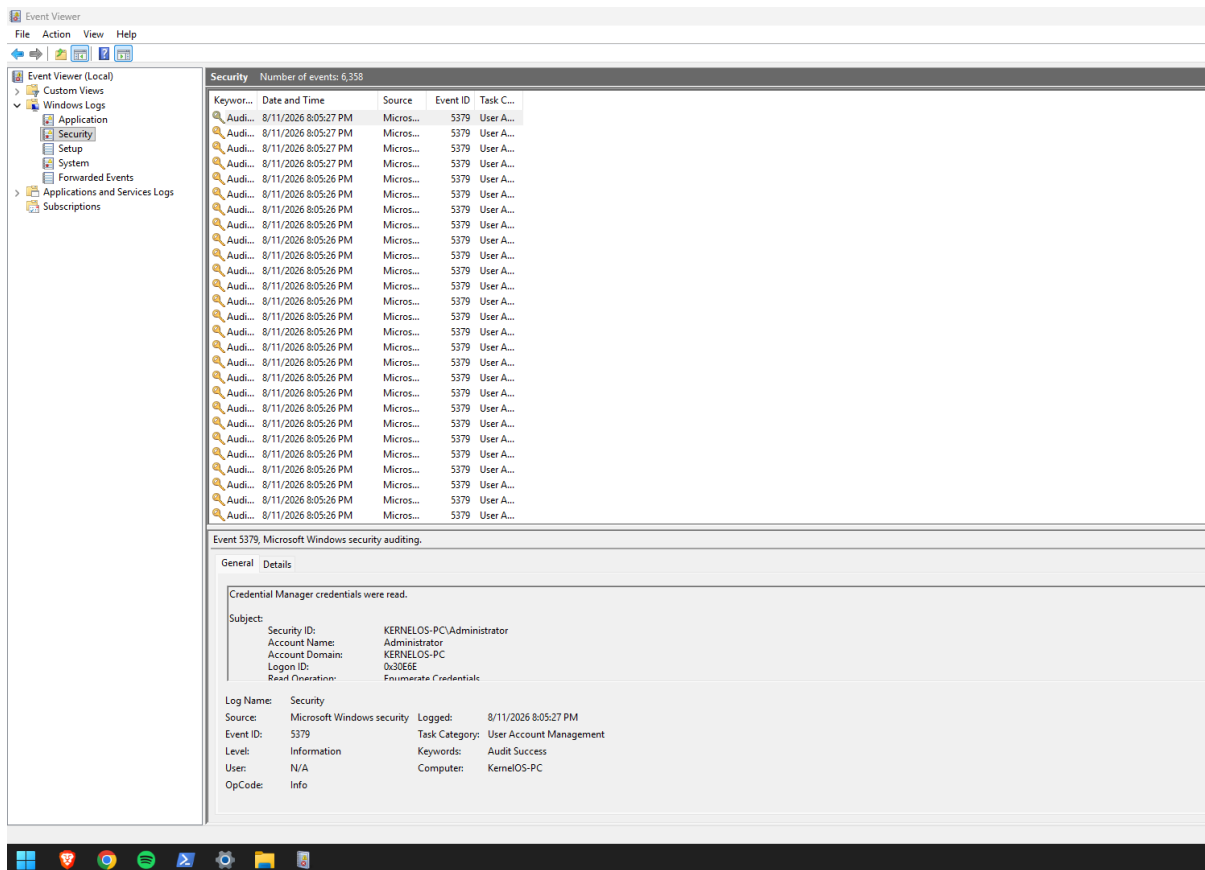
R-04	Unmonitored Third-Party Code: Vulnerabilities in open-source software dependencies introduce supply chain entry points.	4	4	16 (High)	Mandate Software Bill of Materials (SBOM) tracking and continuous automated vulnerability scanning in software pipelines.	4 (Low)
R-05	Excessive Access Rights: Over-privileged database accounts allow bulk, unencrypted exfiltration of PII records.	3	5	15 (High)	Enforce least-privilege access, Just-In-Time privilege escalation, and real-time Database Activity	3 (Low)

6. COMPONENT 5: COMPLIANCE, INCIDENT RESPONSE, AND TECHNICAL CONTROLS

Regulatory Alignment and Breach Notification Standards

To comply with global data protection mandates (GDPR, DORA, NIS2), the enterprise enforces statutory breach disclosure timelines:

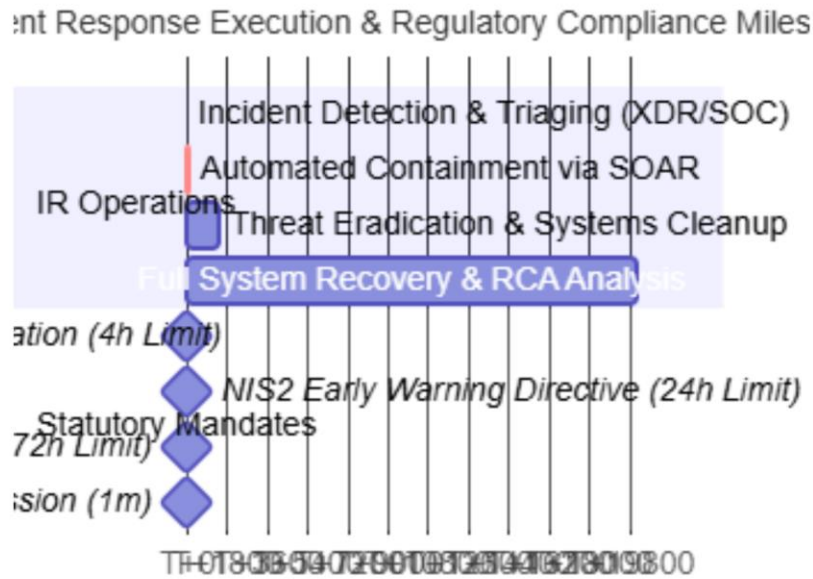
- **GDPR (Articles 33 & 34):** Personal data breaches must be reported to the relevant Supervisory Authority within **72 hours** of discovery. Affected individuals must be notified without undue delay if the incident poses a high risk to their privacy rights.
- **Digital Operational Resilience Act (DORA – EU 2022/2554):** Financial institutions must submit an initial notification of major ICT incidents to regulatory authorities within **4 hours** of classification, followed by an intermediate report within 72 hours and a final report within 1 month.
- **NIS2 Directive (EU 2022/2555):** Essential and important entities must issue an "early warning" notification within **24 hours** of detection a significant cyber threat of incident, followed by a full report within 72 hours.



Incident Response (IR) Lifecycle

Aligned with **NIST SP 800-61 Rev. 2**, the incident management lifecycle includes four structured phases:

1. **Preparation:** Establish pre-authorized SOAR playbooks, maintain hardened system baselines, perform bi-annual tabletop drills, and test immutable backups.
2. **Detection and Analysis:** SOC analyst evaluate alerts from XDR, SIEM, and UEBA engines to classify and triage incidents within 15 minutes of occurrence.
3. **Containment, Eradication, and Recovery:**
 - a. *Containment:* Automated SOAR playbooks isolate affected endpoints, revoke active user session tokens, and deploy WAF filtering rules.
 - b. *Eradication:* Malicious files, compromised accounts, and rogue persistent services are purged from the network environment.
 - c. *Recovery:* Systems are restored from verified clean baselines using immutable backups, with full functionally validated prior to reconnecting to production network zones.
4. **Post-Incident Activity:** A formal root-cause analysis is conducted within 14 days to refine incident playbooks, update security policies, and enhance monitoring capabilities.



Technical Controls and Impact Reduction

The technical safeguards built into this programme address the specific points of failure identified in the Equifax breach:

- **Automated PKI Management:** Eliminates visibility gaps by ensuring TLS decryption certificates remain valid, allowing continuous network traffic inspection.
- **XDR and SOAR Orchestration:** Reduces Threat Time from months to minutes through automated cross-domain correlation and rapid endpoint containment.
- **ZTNA and Micro-segmentation:** Restricts lateral movement, preventing compromised web applications from directly accessing internal consumer databases.
- **Inline DLP and Database Activity Monitoring:** Detect and interrupts bulk data exfiltration attempts in real time, preventing unauthorized data extraction even if credentials are compromised.

CONCLUSION

The cybersecurity programme established in this report provides a comprehensive strategy for protecting enterprise information assets in complex digital environments. By critically evaluating Zero Trust principles and hybrid workforce protection in Task 1, this paper demonstrated the limitations of traditional perimeter-based security in modern cloud environments.

Task 2 applied these technical and architectural principles to address the root governance and technical failures of the 2017 Equifax breach. By embedding the **NIST Cybersecurity Framework 2.0**, enforcing strict patch SLA policies, maintaining complete asset visibility, deploying automated PKI certificate management, and aligning with regulatory frameworks including GDPR, DORA, and NIS2, this program establishes a proactive security posture designed to **Anticipate, Protect, Detect, and Automatically Respond** to modern cyber threats.

REFERENCES

- Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Mhiqani, M. N. (2022). A survey on Zero Trest security model: Challenges, recent advances, and future trends. *IEEE Access*, 10, 124162-124188.
- Buckley, J., & Nurse, J. R. (2023). Cyber security breaches and organizational governance: Analyzing executive accountability. *Computers & Security*, 129, 103192.
- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1-88.
- European Union. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). *Official Journal of the European Union*, L 333, 1-79.
- European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*, L 333, 80-152.
- Gartner. (2023). Magic quadrant for single-vendor SASE. Gartner Research.
- National Institute of Standards and Technology. (2020). Zero Trust Architecture (NIST Special Publication 800-207). U.S. Department of Commerce.
- National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Special Publication 800-54). U.S. Department of Commerce.
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *NIST Special Publication*, 800-207.
- Syrenkyi, A., & Bakhshi, T. (2023). Securing the hybrid workforce: Critical analysis of SASE and ZTNA paradigms. *Journal of Information Security and Applications*, 75, 103481.
- U.S. House of Representatives Committee on Oversight and Government Reform. (2018). The Equifax data breach. 115th Congress, 2nd Session.