CROWDSTRIKE

Information Security Program

10.08.2024

Created by: Group 5

- Harika Aakula
- Karthik Reddy Guntakandla
- Madhusudan Kummari
- Sai Nikhil Reddy Kura
- Namo Bhavani Maganti
- Dhanesh Reddy Pulagam
- Harshith Shivaswamy

1. Information Security Program Strategy

Mission	To potentially identify and detect attacks to safeguard CrowdStrike's security solutions and assets against evolving and constant cyber threats.
Vision	To create innovative solutions in a rapidly evolving digital world, empowering CrowdStrike to operate confidently while becoming a global cybersecurity leader.
Goals	• Ensure compliance with security frameworks. • Protecting CrowdStrike reputation • Monitoring and responding to the threats across the entire company network

Strategic Objectives and Outcomes

Objectives	Description	Expected Outcomes
Enhance Threat intelligence and response capabilities	Increase the ability to identify, analyse and respond to advanced threats	• Enhanced accuracy of threat detection • Improved Incident response • Time to detect and time to respond potentially reduces
Boost cloud security posture and robustness.	Improve cloud security practices to safeguard against potential attacks and vulnerabilities in cloud settings.	• Potential decrease in risk of cloud breaches • Enhanced visibility into cloud activity • Improved compliance with cloud security standards with Frameworks
Enhance Identity and Access Management Security	Strengthening our IAM practices will prevent unauthorized access	• Minimal Lateral Moment • Improved protection against Credential theft • Reduction in phishing and social engineering attacks

Strategic Initiatives

Strategic Initiatives	Description	Related Strategic Objective	Expected Outcomes
Investing in advanced threat intelligence	Expanding partnerships with technology companies leveraging AI machine learning to identify emerging threats	Enhance Threat intelligence and response capabilities	Helps in developing more efficient and effective detection and threat response strategies
Adopt a trusted Zero trust approach and Implement Cloud-native security control	Trust no one or anything and utilise cloud-native security tools such as firewalls, encryption and intrusion detection system	Boost cloud security posture and robustness	• Decrease the risk of unauthorised access to the cloud • Protect cloud workload from vulnerabilities that target specific cloud environment
Implementing Strong MFA (Multi-Factor Authentication) and Educating employees	Adding an extra layer of security. Educating employees on social engineering	Enhance Identity and Access Management Security	• Potential reduction in social engineering attacks • Increase in Employee awareness

Security Framework

Selected Framework: Control Framework- NIST 800-53, Program Framework- NIST CSF, Risk Framework- NIST 800-39
Explanation of Choice: The frameworks selected for CROWDSTRIKE include a combination of control, program and risk frameworks. The primary reason for selecting NIST 800-53 is that it helps ensure security controls, and it perfectly aligns well with federal standards such as access control, incident responses and system protection, which satisfies the company's mission and can be tailored to meet specific needs (Force, 2017). Whereas NIST CSF provides a mixed blend approach in managing cybersecurity risk in parallel with the business objectives, these frameworks' core functions identify, protect, detect, respond, and recover, providing a comprehensive approach which allows our organization to prioritize efforts based on most critical risks (Pascoe et al., 2024). CROWDSTRIKE. NIST 800-39 framework has been chosen as it ensures the integration of risk management into every aspect of our core operations and services, from high-level strategy to specific information system levels (Ross, 2011). It is essential for our organization as it survives in a complex and dynamic environment of constantly evolving cybersecurity threats.

2. Risk Appetite Statement

Risk Type	Risk Appetitive Statement	Risk Level Explanation
Data Security Risk	CrowdStrike has no tolerance towards data breaches, especially breaches that involve unauthorised access or the theft of sensitive client data. As Crowd Strike's cybersecurity leader, we prioritise data integrity and confidentiality and implement robust protection measures all over the systems.	Risk: Credential theft and breaches are driven by identity-based attacks Impact: It can cause significant financial loss and reputation damage Focus: To follow strong IAM management and to improve monitoring and detection of abnormal behaviour to help prevent breaches
Strategic Risk	CrowdStrike is willing to accept a considerable amount of strategic risk while adopting new technologies and considering that taking risks is needed to drive innovation and maintain a competitive edge. Anyway, risks linked with security vulnerabilities need to be mitigated to avoid disruptions.	Risk: It probably includes security gaps or any misconfigurations in emerging technologies Impact: This may lead to vulnerability exploitation, further affecting business growth Focus: Aiming to secure the adoption of new technologies requires careful planning and risk management.
Operational Risk	CrowdStrike has a low tolerance for operational disruptions, as incidents like cloud security misconfigurations can lead to service interruption and downtime. Our organisation is aimed toward maintaining operational resilience in growing cloud complexities.	Risk: Certain risks, such as faulty software updates which happened in recent Microsoft outage incidents or cloud misconfigurations, can lead to disruptions Impact: Due to these risks, CrowdStrike loses the ability to deliver its core services, which impacts reputation and financial damage. Focus: Ensure operational continuity through robust cloud security control methods
Financial Risk	CrowdStrike has little tolerance for financial risk as the company recognises that robust cyber security measures come at a considerable price. Moreover, organisations seek to minimise financial exposure to cyberattack incidents through vital prevention and detection mechanisms.	Risk: This may involve the costs of responding to cyberattacks, especially identity-based attacks or breaches. Impact: These can cause legal penalties and significant financial strain because of incident response and remediation efforts. Focus: Preventing financial burden by improving early detection and incident response capabilities

3. Risk Assessment

Specific Risk 1: Data security Risk: Credential theft and data breaches		
Risk description	Malicious actors can exploit credentials and access sensitive client and internal information unauthorisedly.	
Risk score		**Reasons for the score given**
Impact score	High	It can lead to significant financial, legal, and reputational damage
Likelihood score	Medium	Credential theft has likely become more sophisticated, and the risk of successful identity theft attacks may increase.
High-level mitigation strategy		
CrowdStrike can focus on implementing stringent identity verification followed by Multifactor authentication, and implementing robust IAM Policies can mitigate those risks. Further, continuous monitoring of access behaviours is advised.		

Risk 2: Strategic Risk: Container Security Misconfigurations		
Risk description	Malicious actors or hackers targeting poorly configured container environments	
Risk score		**Reasons for the score given**
Impact score	Medium	Security gaps in containers can be exploited while impacting operations, but these impacts are often contained in specific services or workloads. Overall, the business might not experience severe disruption.
Likelihood score	Medium	As the use of containers is increasing day by day, the chances for container misconfiguration slightly increase.
High-level mitigation strategy		
CrowdStrike can focus on using automated configuration tools and conducting regular or quarterly reviews on security standards. This may improve container security awareness.		

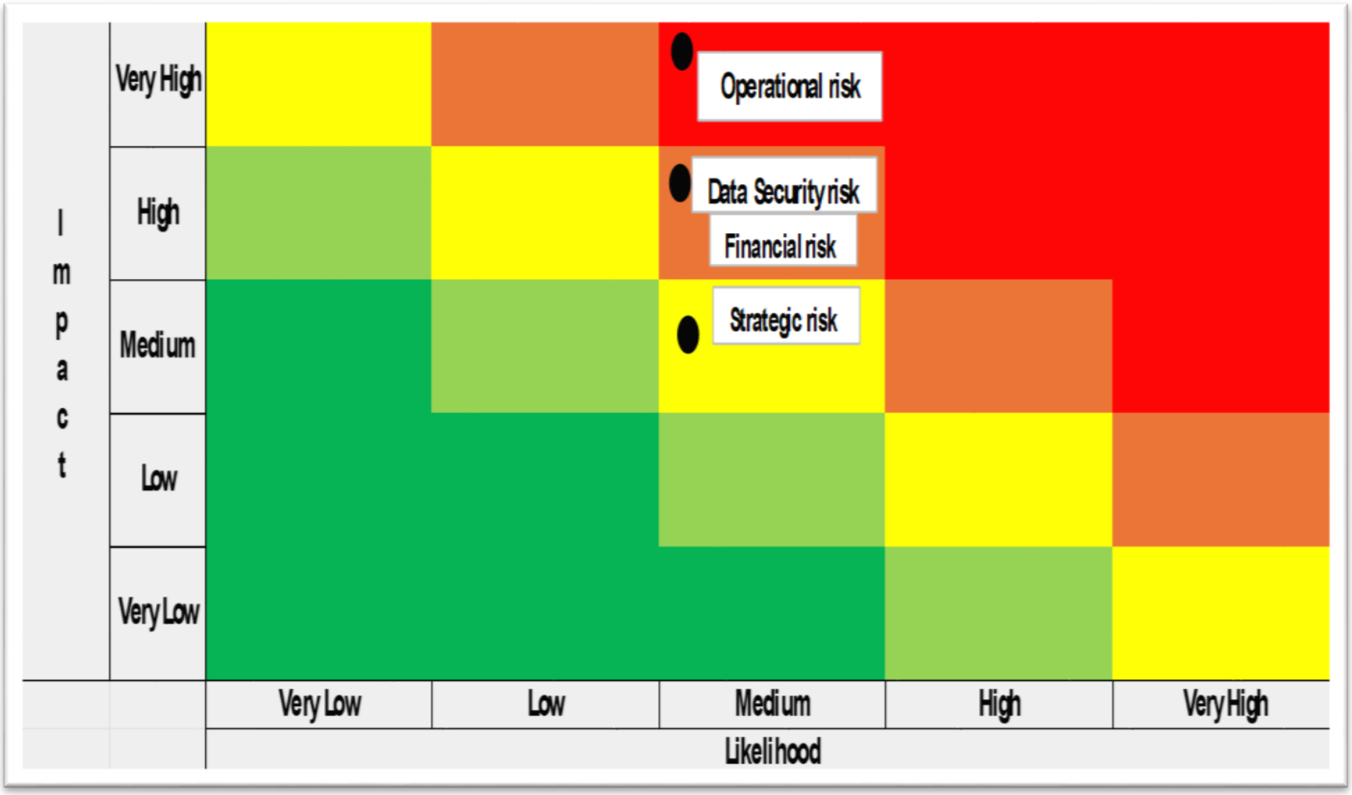
Risk 3: Operational Risk: Cloud Misconfigurations		
Risk description	Malicious actors can access unauthorised ways due to poor cloud configurations, leading to service interruptions.	
Risk score		**Reasons for the score given**
Impact score	Very High	Misconfigurations can lead to severe operational disruptions and data loss.
Likelihood score	Medium	Though misconfigurations are common, they can be mitigated with robust processes.
High-level mitigation strategy		
CrowdStrike can perform regular audits and deploy automated cloud configuration tools while closely monitoring the cloud environments.		

Risk 4: Financial: Huge costs from Identity-based Attacks		
Risk description	Financial burdens to responding to increasingly sophisticated identity-based attacks can lead to costs in mitigation strategy, legal fees, and penalties.	
Risk score		**Reasons for the score given**
Impact score	High	These attacks lead to costly disruptions and compliance fines
Likelihood score	Medium	There has been a significant increase in identity-based attacks that increase the likelihood of financial burdens.
High-level mitigation strategy		
Implementing early threat detection, enhancing the threat monitoring system, and having a robust incident response plan can limit financial losses.		

4. Heat Map & Priorities

Risk Priority	Risk Name
1	Operational risk
2	Data security risk
3	Financial risk
4	Strategic risk

Heatmap on Risk Assessment

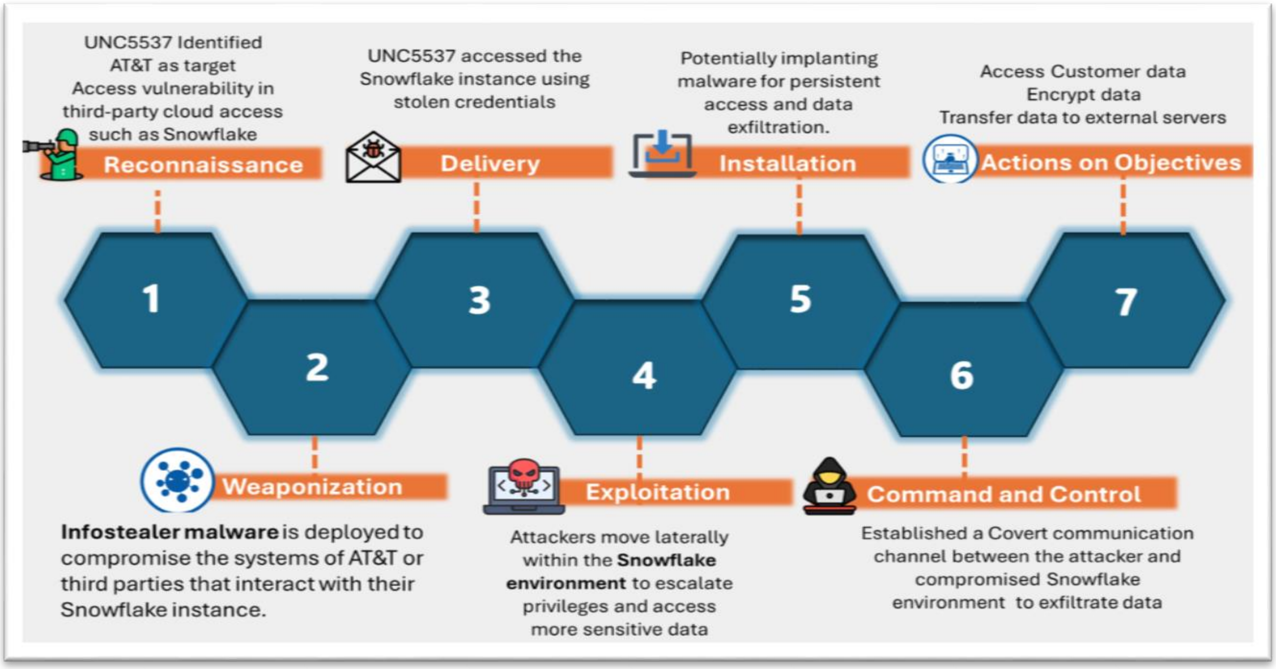


5. Security Incident Mapping

Selected incident: AT&T data breach incident- Unlawful access to call and Text records

Incident Summary: AT&T discovered that hackers illegally downloaded their customer's data on a third-party cloud platform (Snowflake) and were able to exfiltrate sensitive information (Vasquez, 2024). The downloaded data included phone call records, text messages, and mobile network operators' customers using AT&T’s network. The incident has been highlighted on the news as of April 2024, and as per records, it is said that the breach occurred between May 1, 2022, and October 31, 2022, and some additional from January 2, 2023 (AT&T, 2024). The data identifies phone numbers that interacted with AT&T and MVNO cellular numbers, including landline numbers. Cell site ID numbers were also included for a subset of records. However, the breach did not expose the content of calls or texts, timestamps, Social Security numbers, or other personally identifiable information (AT&T, 2024). AT&T warned that names could potentially be linked to phone numbers using publicly available tools.

Mapped Cyber Kill Chain diagram



Reconnaissance: UNC5537 Identified AT&T as target Access vulnerability in third-party cloud access such as Snowflake

Weaponization: **Infostealer malware** is deployed to compromise the systems of AT&T or third parties that interact with their Snowflake instance.

Delivery: UNC5537 accessed the Snowflake instance using stolen credentials

Exploitation: Attackers move laterally within the **Snowflake environment** to escalate privileges and access more sensitive data

Installation: Potentially implanting malware for persistent access and data exfiltration.

Command and Control: Established a Covert communication channel between the attacker and compromised Snowflake environment to exfiltrate data

Actions on Objectives: Access Customer data Encrypt data Transfer data to external servers

Analysis Using the Cyber Kill Chain Diagram

1. Reconnaissance

Description: Attackers (UNC5537) attacked AT&T by successfully identifying access vulnerabilities in the third-party cloud providers, Snowflake particularly. (Lennon, 2024)

Action in the breach: Attackers targeted third-party cloud providers' weak entry points by finding vulnerabilities in their environment.

2. Weaponisation

Description: Infostealer malware was deployed to infect AT&T systems and third-party systems.

Action in the breach: Attackers utilized malware to extract credentials, data files and certain crucial information from AT&T and Snowflake platforms.

3. Delivery
Description: Attackers accessed the Snowflake instance via compromised credentials.
Action in the breach: Attackers can access by likely using stolen credentials and thereby obtained through phishing or any other method.

4. Exploitation
Description: The attackers moved within the Snowflake environment to obtain higher privileges
Action in the breach: Gaining more privilege has led attackers to access the AT&T network to reach sensitive data with the Snowflake environment

5. Installation
Description: The attackers installed malware to maintain a long-term presence and to steal data.
Action in the breach: The intruder installed unauthorised code for maintaining persistent access and for data exfiltration from the Snowflake environment

6. Command and Control
Description: The attackers created a secret channel to pull information out.
Action in the breach: Communication channel allowed for continuous data transfer involving confidential customer or corporate data

7. Actions on Objectives
Description: The attacker also drilled into the company's customers' records
Action in the breach: The objective has been achieved by stealing and encrypting customer-sensitive data and transferring it to an external server.

Conclusion:
AT&T also owns a multi-stage attack, where hackers exploit vulnerable links in the third-party cloud storage (Snowflake). The Cyber Kill Chain model describes each step, highlighting the need for robust third-party access controls to prevent breaches.

Potential Negative Impacts on Our Organization:

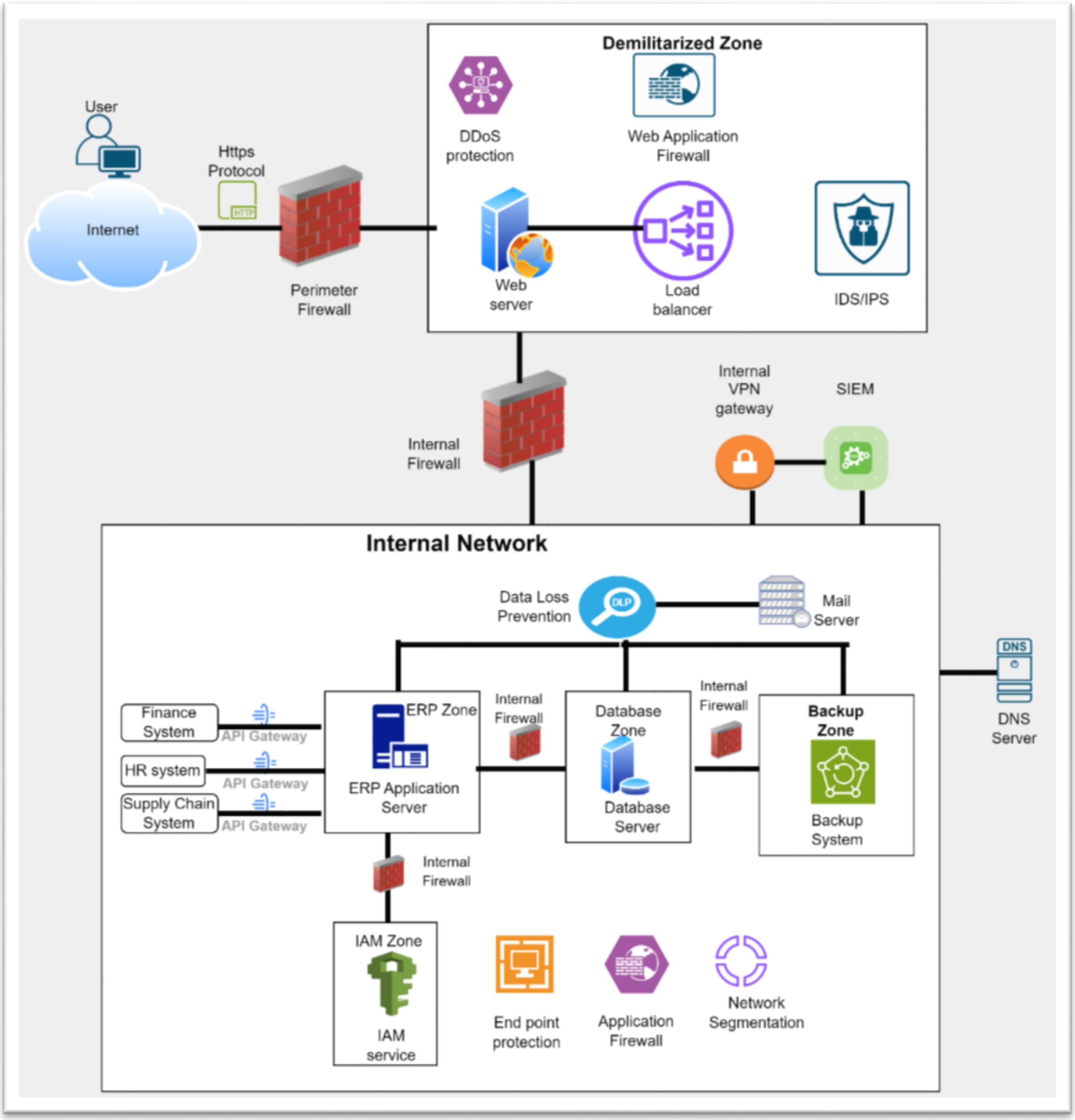
Reputation loss and Customer Trust: A similar breach as of AT&T would significantly lead to the loss of trust and damage CrowdStrike's reputation (JUST SOLUTIONS, INC., 2024).

Financial Loss: A data breach within our company, which can involve a breach of sensitive data such as client information, can result in regulatory fines, lawsuits and the cost of remediation (JUST SOLUTIONS, INC., 2024).

Competitive disadvantage: Our company's mission is to stop breaches if a breach has occurred due to vulnerabilities, making competitors utilise the opportunity to lure clients (Whited, 2024).

Core Operational disruption: CrowdStrike's core operations would be impacted, delaying service delivery and customer support and impacting further developments (Whited, 2024).

6. Secure Architectural Design and Diagram



Analysis of Technology Choices:

In the network diagram provided, one can see a well-constructed and well-protected on-premises ERP system. The selected technologies reflect industry standards in a way that provides adequate data security while facilitating operations.

Perimeter Security:

Perimeter firewall: Performs functions to protect the organisation against threats from outside the company.
DMZ: Restricts accessibility of front-end servers, minimising the target area (NIST et al.: 2024).

Network Segmentation:

Internal firewall: Splits the network into smaller parts, reducing the consequence of the break-in (CIS Controls, 2024).
Network segmentation: More limitations exist on the availability of proposed resources, thus improving protective capabilities (CIS Controls, 2024).
Application Security:

WAF: Guards against common deficiencies noticed in web applications (NIST et al., 2024).
Endpoint protection: Protect the hardware and software from dangerous programs in the network (NIST et al., 2024).

Data Security:

DLP: The tool effectively mitigates the exfiltration of sensitive information (NIST et al., Version 1.2, 2024).
Backup system: It also protects data in a disaster (NIST et al., 2024).

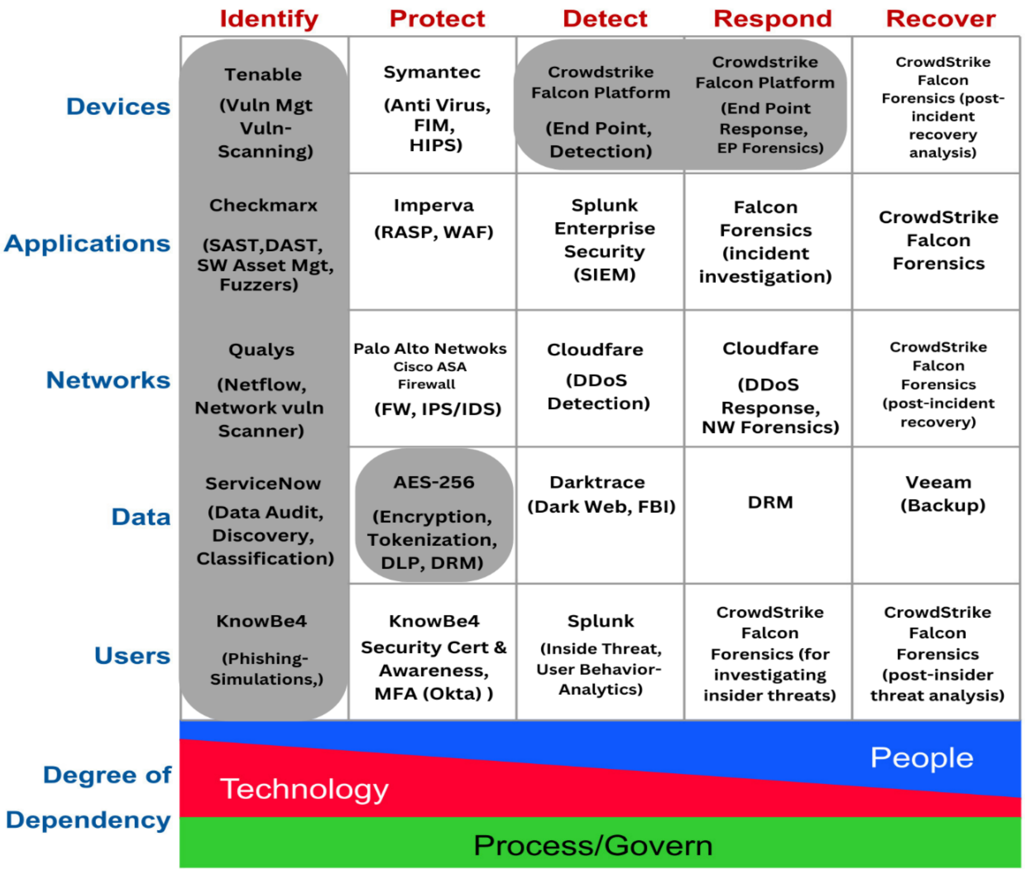
IAM:

IAM service: Controls the user’s access to the network resources to deny everyone but authorised personnel access (NIST et al., 2024).

Network Monitoring:

SIEM: Remembers and stores logs of activities and events and provides real-time security monitoring with the help of the NIST Cybersecurity Framework in 2024.

7. Cyber Defense Matrix



	Identify	Protect	Detect	Respond	Recover
Devices	Tenable (Vuln Mgt Vuln-Scanning)	Symantec (Anti Virus, FIM, HIPS)	Crowdstrike Falcon Platform (End Point, Detection)	Crowdstrike Falcon Platform (End Point Response, EP Forensics)	CrowdStrike Falcon Forensics (post-incident recovery analysis)
Applications	Checkmarx (SAST,DAST, SW Asset Mgt, Fuzzers)	Imperva (RASP, WAF)	Splunk Enterprise Security (SIEM)	Falcon Forensics (incident investigation)	CrowdStrike Falcon Forensics
Networks	Qualys (Netflow, Network vuln Scanner)	Palo Alto Netwoks Cisco ASA Firewall (FW, IPS/IDS)	Cloudfare (DDoS Detection)	Cloudfare (DDoS Response, NW Forensics)	CrowdStrike Falcon Forensics (post-incident recovery)
Data	ServiceNow (Data Audit, Discovery, Classification)	AES-256 (Encryption, Tokenization, DLP, DRM)	Darktrace (Dark Web, FBI)	DRM	Veeam (Backup)
Users	KnowBe4 (Phishing-Simulations,)	KnowBe4 Security Cert & Awareness, MFA (Okta))	Splunk (Inside Threat, User Behavior-Analytics)	CrowdStrike Falcon Forensics (for investigating insider threats)	CrowdStrike Falcon Forensics (post-insider threat analysis)

Cyber Defense Matrix: Technology Breakdown: Alignment with NIST Functions

Devices:

Tenable (Vuln et al.): This tool assists in pinpointing areas of risks in various devices, such as servers, workstations, etc. It correlates to the NIST Identify function by giving an initial outlook of the security state of all the devices used in the organisation.

CrowdStrike Falcon Platform: This product helps CrowdStrike with real-time Endpoint detection, threat intelligence, automated incident response with forensic data, and incident recovery analysis after a cyber threat event. These aspects perfectly fit the NIST Detect, Respond, and Recover functions.

Applications:

Checkmarx (SAST, DAST, SW Asset Mgt, Fuzzers): Checkmarx is an application for source code analysis to define the weak points of the software. This directly relates to the NIST Identify function, which provides information on the threats bound to applications.

Splunk Enterprise Security (SIEM): This platform combines and performs analysis on data for threat detection, and it perfectly fits in the NIST Detect function

Falcon Forensics (Incident Investigation): This product of CrowdStrike facilitates application incident investigation, and its resolution aligns with the NIST response function.

Networks:

Qualys (NetFlow, Network vuln Scanner): Qualys offers network flow analysis and network vulnerability scans that would determine threats from the networks. It relates well to the NIST Detect function, as it continuously scans the network for any signs of malicious activity and conducts vulnerability assessment.

CloudFlare(DDos Detection and Response): Identifying and responding while mitigating DDoS attacks fits the NIST Detect and Respond function.

CrowdStrike Falcon Forensics: Facilitating incident analysis, detecting the attacker's motive behind accessing networks and recovery relating well with NIST Recover function

Data:

ServiceNow (Data et al.): The use of Data Management features in ServiceNow aims to enable organisations to identify the data they hold and categorise the data according to the type of risk involved in processing it. It conforms to the NIST Recover function as it helps recover data and ensures it is managed correctly.

Darktrace: Utilizing AI technology helps monitor insider threats and prevents data breaches. This fits well with the NIST Detect Function

Users:

KnowBe4 (Phishing Simulations): What others do is KnowBe4 offers users the means to practice phishing simulations that should make them aware of existing threats. It can be aligned with the NIST Protect function as this approach can minimise human mistakes, which create security compromises.

Splunk (User Behavior Analytics): Constantly monitoring for insider threats caused due to user activity goes well with NIST Detect Function

Falcon Forensics (Insider Threat Investigation): Investigates insider threats involving user activity. This aligns with the NIST Respond function.

Technology:

Symantec (Anti-Virus, FIM, HIPS): Symantec offers solutions such as antivirus, file integrity monitoring and host intrusion prevention to protect devices and applications from malware and prevent unauthorised access. That corresponds to the NIST Protect function because it has measures to protect systems and data.

Imperva (RASP, WAF): Imperva provides customers with the runtime application self-protection and web application firewalls to defend their application against the remaining attacks. It contributes to the NIST Protect function, protecting the applications from unauthorised access.

Palo Alto Networks Cisco ASA Firewall (FW, IPS/IDS): This one offers a shield against network warfare, which is common in computer networking. It supports the NIST Protect function by ensuring traffic control and bar access to unauthorised persons.

AES-256 (Encryption), Tokenization, DLP, and DRM are employed to enforce data confidentiality and integrity. They are in line with the NIST Protect function by protecting data safely.

Process/Govern:

NIST Cybersecurity Framework: The NIST CSF guides establishing, conducting, and evaluating a cybersecurity program. This is because it supports all five NIST functions as a framework for managing cybersecurity risks.

People:

KnowBe4 (Security Cert & Awareness): KnowBe4 offers security certification and awareness training to enable users to increase their security knowledge and avoid security malpractices. It aligns with the NIST Protect function because it will make the users more conscious, thus eliminating accidental mistakes.

8. Asset Inventory

Hardware Inventory	
Hardware categories	Department ownership
1. Mobile Phones & Sim Cards	Facilities Management
1. Servers	IT Department
2. IAM Devices	Security Department
3. Storage Devices	IT Department
4. Printers & Scanners	Facilities Management
5. Desktop Computers & Laptops	IT Department
6. Security Cameras	Security Department
7. Network Devices	IT Department
8. Projectors	Facilities Management
9. Backup Power Supply (UPS)	Facilities Management

Software Inventory		
Software names	Business Purpose	Department ownership
1. Microsoft O365	Collaboration, Communication & Document Management	IT Department
2. CrowdStrike Falcon	Threat Detection & Endpoint Security	Cyber Security Department
3. Salesforce	CRM (Customer Relationship Management)	Sales & Marketing
4. Jira	Issue Tracking & Project Management	IT Department
5. SAP ERP	Enterprise Resource Planning & Operations	Finance/Supply Chain Department

Data Classification

- **Data Classification 1: Physical Data**
  Information is stored in physical formats like paper files or hardware.
- **Data Classification 2: Log Data**
  Records of system activities, transactions, and user interactions.
- **Data Classification 3: Sensitive Data**
  Highly confidential information requiring strict access control.

9. Security Regulations and Certifications

Security Regulations and Their Impact

- **Regulation 1: General Data Protection Regulation**
  - GDPR applies to organizations that handle EU citizen data, and CrowdStrike, due to its presence in the EU, should adhere to GDPR. This regulation requires safeguarding sensitive data, such as personal, online, and biometric information, holding data controllers and processors equally liable (Staff, 2023). CrowdStrike should implement strong data protection measures and maintain GDPR compliance for internal processes and third-party data processors, reducing the liability risks connected with data handling for EU residents.
- **Regulation 2: Federal Information Security Management Act**
  - CrowdStrike, a leader in cyber security, offers its services to various industries, including federal organizations. Considering this, our company needs to be compliant with FISMA. These regulations demand that federal agencies and contractors maintain comprehensive security procedures, perform regular risk assessments, and establish security and incident response lifecycle policies (Staff, 2023). This regulation impacts our company by requiring robust security protocols, periodic policy verification, and continuous planning for maintaining contracts.
- **Regulation 3: California Consumer Privacy Act**
  - CrowdStrike is a company that originated in the United States, serving people around America and people hailing from California. It is crucial for the company to obey California Consumer Privacy Act (CCPA) regulations. This regulation gives customers substantial data management rights involving access, deletion and disclosure rights, including the opportunity to sue the company for privacy infractions (Staff, 2023). This regulation impacts Crowdstrike in preserving and reacting to data requests linked especially to customers in California, such as identifiers, geographical location, internet activity, and other personal data. This regulation will help implement processes for maintaining customer rights and data transparency.

Industry Certifications

CrowdStrike considers obtaining ISO 27001 and SOC 2 certifications critical as the mission highlights protecting security solutions from emerging cyber threats. ISO 27001 provides a structured framework for developing an Information Security Management System (ISMS) and improving threat intelligence and response capabilities through comprehensive risk assessments and robust controls (Alhajeid, 2024). It perfectly aligns with CrowdStrike's objective of operating confidently in a changing digital context. On another note, SOC2 certification will ensure robust security practices are incorporated in protecting sensitive customer information (Alhajeid, 2024)., aligning with the company's goal of threat monitoring and compliance with frameworks such as NIST 800-53 and NIST 800-39, which emphasise rigorous security standards. These certifications indicate CrowdStrike's dedication to security best practices and help defend the company image, which is critical for achieving strategic objectives.

10. Incident Response Plan

Incident Name: AT&T data breach incident- Unlawful access to call and Text records

Incident Response Team Stakeholders and Responsibilities

Internal Team:

- **CSO/CISO:** Communicate the incident with the board/C-suite while ensuring the alignment with security posture and business objectives (CROWDSTRIKE INCIDENT RESPONSE, n.d.).
- **Incident response manager:** Coordinates between different teams and team members
- **Security operations Centre team**: Detect the breach, isolate the contaminated third-party system, and prevent the attack from spreading.
- **Threat Intelligence team:** Real-time insights into attacker methods and motives, helping the incident response team prioritize actions.
- **Forensic Team:** Analyses the breach and gathers evidence on attack methods
- **PR team:** Manage external communication and maintain trust of customers/clients
- **Legal and compliance team** addresses the legal consequences and ensures compliance with rules and regulations (CROWDSTRIKE INCIDENT RESPONSE, n.d.).

External Team:

- **Third-party vendors:** Collaborate to address vulnerabilities and protect external systems.
- **Law Enforcement:** Investigate cybercrime to identify attackers and take legal action.
- **Regulatory Bodies:** Ensures compliance with data protection guidelines
- **Law Firms:** Protect legal privilege throughout the incident

Incident Reporting

- **C-suite:** Facilitates strategic legal, PR and resource allocation decision-making
- **Clients/Customers:** Informing about breaches and guidance on data protection.
- **Employees/ teams:** Communicate with departments (HR, Finance) for a unified response
- **Insurance Carriers:** Assess insurance claims, financial impacts and remediation costs.

Tools and Technologies for Incident Response

- **CrowdStrike Falcon platform:** Real-time detection and threat visibility within hours of the breach, ensuring rapid detection and response (CROWDSTRIKE INCIDENT RESPONSE, n.d.)
- **Falcon Forensics:** Collects crucial forensic data and gains insights into attackers' action
- **Falcon Real-Time Response:** Remotely respond to incidents, ensuring minimal disruption
- **Falcon Spotlight:** Identify and patch system vulnerabilities and prevent exploiting unpatched systems (CROWDSTRIKE INCIDENT RESPONSE, n.d.).
- **Falcon Overwatch:** Detects lateral moment attacks and prevents data exfiltration efforts.
- **Falcon Identity Threat Detection:** Monitors and identifies compromised credentials, halting privilege escalation.

SLA for Incident Response

- **Downtime:** Minimizing customer impact and restoring regular business operations within 5 hours
- **Detection time:** Detect the threat of compromised access within 1 day
- **Containment Time:** Contain the active threat within 2 days to prevent further data exfiltration
- **Attacker Dwell time:** Reducing the dwell time to less than 2 days to minimize the effect of data compromise.
- **Recovery Time Objective:** Recover systems within 6 hours, especially infected endpoints
- **Recovery Point Objective:** Data recovery from backups no older than 12 hours to minimize data loss and protect integrity.

11. SOC Team and Toolset

SOC Tools

- Security Information and Event Management- Splunk Enterprise Security
- Endpoint Detection and Response- CrowdStrike Falcon Insight
- Threat Intelligence Platform- Anomali Threat stream
- Incident Management System- Splunk On-Call
- Vulnerability Management Tools- Qualyus VMDR
- Security Orchestration, Automation and Response (SOAR)- Splunk Fantom
- Forensic Analysis Tools- CrowdStrike Falcon Forensics
- Extended Detection and Protection- Sentinel One Singularity XDR

SOC Model:

CrowdStrike will adopt an Internal/Dedicated SOC model. The choice has been made considering several strategic factors aligning with the companies offering services and operations and fulfilling the unique demands in this growing digital landscape. CrowdStrike, a leader in Cybersecurity Technology providers, focuses primarily on providing advanced endpoint protection, threat intelligence and incident response through its Falcon Platform. Its SOC model being Internal/Dedicated allows them to utilize their existing technologies and expertise for seamless integration of its security solutions into day-to-day operations. It is beneficial as SOC can use real-time insights from Falcon, thereby increasing the efficiency of Incident Response and Threat Detection. The internal SOC model allows the company to tailor their monitoring and response strategies to specific needs, providing maximum control (IANS Faculty, 2021). This feature will enable CrowdStrike to customize security processes, especially in this evolving landscape of cyber threats. CrowdStrike possesses skilled people in cybersecurity, a critical asset for a successful internal SOC model. It also ensures faster threat detection and response capabilities (Kidd, 2023). Implementing this model involves enormous capital investment, but this ultimately leads to lower operational costs, and this model provides better cost control and predictability (IANS Faculty, 2021). CrowdStrike, which operates on a subscription-based model investing in an internal SOC, aligns with its financial strategy of minimizing recurring costs associated with outsourced services. CrowdStrike, through its internal SOC model, ensures that incident response teams have faster access to threat intelligence data for accurate responses to incidents.

12. Business Impact Analysis (BIA)

Key Application name: ERP (Enterprise Resource Planning) System

Business unit and high-level business processes:
Business Unit: Supply Chain Management, Human Resources, Operations, Finance.
High-level Business Process:
The ERP system connects major operational processes considered important in any organization, such as financial, human resources, purchase, supply chain and inventory. The ERP facilitates organizational communication between departments, supports business resources, and manages real-time data processing for all functions.

Financial impact analysis:
Disruption of an ERP system can severely impact financial operations, causing invoice mismanagement, payroll delays, and supply chain inefficiencies. Financial losses may include lost revenue from halted orders, increased operational costs for recovery, and fines for missing financial standards. Each day of outage could cost up to $500,000.

Operational impact analysis:
A Disruption of an ERP System can severely Impact Operations. Employee work output would be reduced because they cannot have real-time information for decision-making for the company's payroll and Human resource functions; this would imply that operations have to be slowed down, implying that morale will be affected. Referring to the absence of order and account information, customer service performance would be subjected to a growth in dissatisfaction.

Recovery objectives:
Recovery Time Objective (RTO): 4 hours
The system should be restored within 4 hours to prevent severe operational disruptions and financial losses.
Recovery Point Objective (RPO): 12 hour
Data recovery must ensure that the system can be restored to a point no more than 12 hour before the outage to minimize data loss.

Workaround processes:
When an ERP system has failed, one can be able to manage inventory and financial processing using simple excel sheets for some time. Taking turns, the teams can receive emails and use cloud backup access to share updates and perform the most basic tasks. These are usually adopted as ways of reducing interruption in the man time till the ERP system can be fixed

13. Data Classification Policy

Purpose: To establish a framework to Identify, handle, Classify and secure the data within CrowdStrike. Ensuring that data is protected according to its risk and sensitivity, maintaining legal compliance & internal security standards.

Scope: The policy covers all data formats within the infrastructure, including proprietary data, customer records and threat intelligence, bound to all the employees, contractors and third- parties who interact with the data in any format.

Classification Categories:

1. **Physical Data:** Refers to tangible documents or records, such as printed paper files, that contain sensitive information.
2. **Log Data:** Stored in IT Systems such as records of system activities, transactions, user interactions, & audit trails, generated by systems applications, or network devices.
3. **Sensitive Data:** Confidential information that requires strict access control. including (PII), financial records, trade secrets, threat intelligence reports & intellectual property.

Data Handling:

1. **Physical:** Store in access-controlled areas (lockable cabinet). Use secure printing, Disposal of documents after its lifecycle via shredding or other safe destruction.
2. **Log:** Secure data by encryption during transmission & storage. Regular backups. Retain & review logs based on the retention policies to detect unauthorized access attempts.
3. **Sensitive data:** Strong encryption & data masking. stringent access controls including MFA & should be audited regularly. Requires explicit management authorization/approval for accessing & external sharing of data.

Roles and Responsibilities:

- **IT and Security Teams:** Implement data protection technologies, monitor sensitive & log data to ensure secure handling data. Enforce compliance with data protection measures.
- **Managers:** Enforce policy adherence within their teams and make sure they follow policy and report violation rules, ensuring proper handling of classified data by
- **All personnel:** Follow the data storage, access, & disposal rules to ensure data is handled in accordance with its classification.

Data Discovery and Monitoring:

Periodically assess and categorize data to verify correct classification & adherence to handling policy. Monitor data activity for illegal access attempts. To avoid data leaks or breaches, continuously scan systems for critical data, and impose supervision.

Data Lifecycle Management:

Classify data during reation & asses regularly. Ensure physical data is securely stored, & the log data is retained as per requirements and sensitive data is encrypted throughout its lifespan.

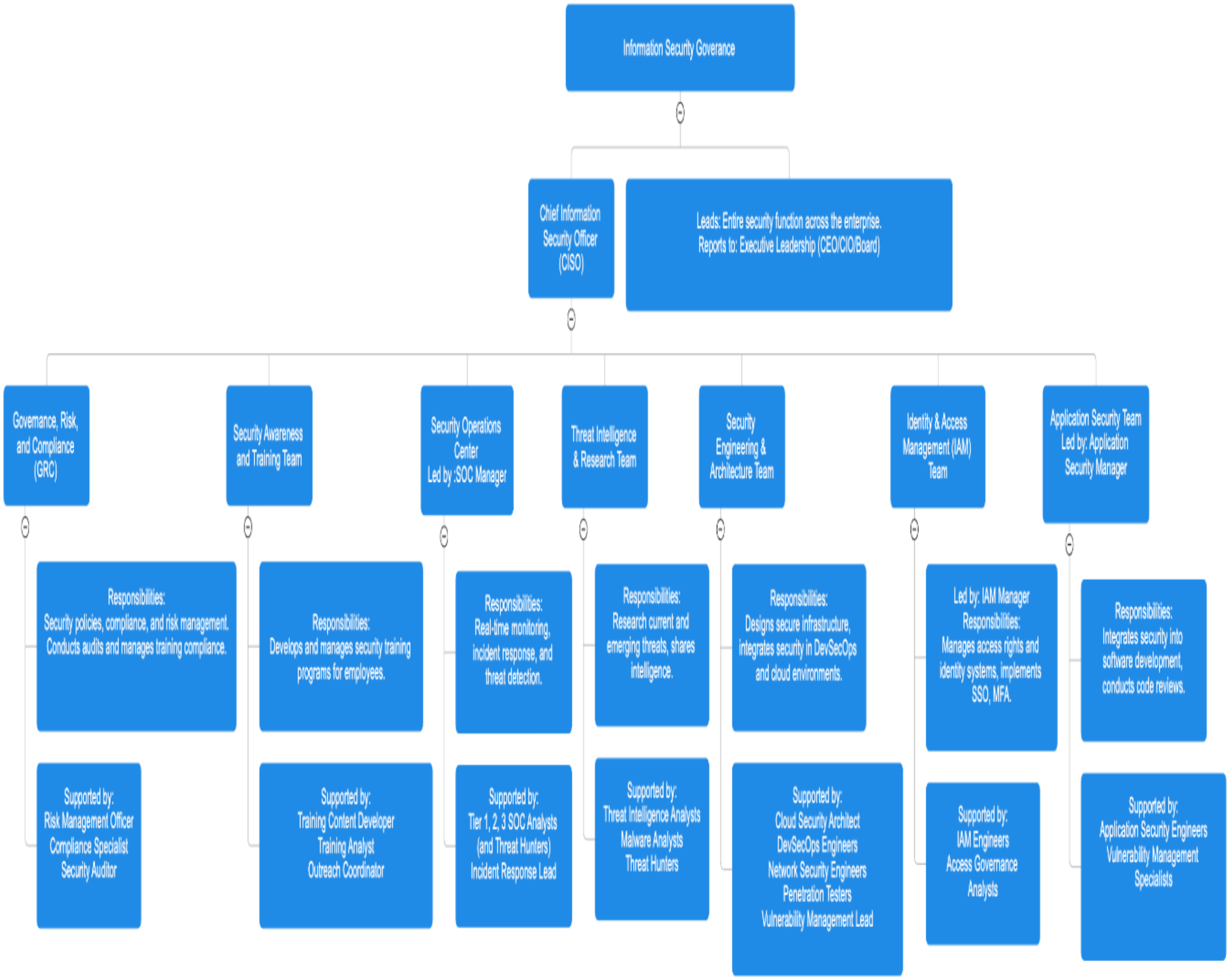
Training:

Employees and staff must complete yearly training. This involves knowing the risks associated with mishandling of data protection guidelines. The training should create awareness by emphasizing the importance of securing sensitive info, according to established protocols.

Policy Violation:

Non-Compliance with this policy may result in disciplinary action, termination and legal implications, for both the individual and the company if data protection laws are broken.

14. Security Team Organizational Structure



Information Security Goverance

Chief Information Security Officer (CISO)

Leads: Entire security function across the enterprise.
Reports to: Executive Leadership (CEO/CIO/Board)

Governance, Risk, and Compliance (GRC)

Responsibilities:
Security policies, compliance, and risk management.
Conducts audits and manages training compliance.

Supported by:
Risk Management Officer
Compliance Specialist
Security Auditor

Security Awareness and Training Team

Responsibilities:
Develops and manages security training programs for employees.

Supported by:
Training Content Developer
Training Analyst
Outreach Coordinator

Security Operations Center
Led by :SOC Manager

Responsibilities:
Real-time monitoring, incident response, and threat detection.

Supported by:
Tier 1, 2, 3 SOC Analysts
(and Threat Hunters)
Incident Response Lead

Threat Intelligence & Research Team

Responsibilities:
Research current and emerging threats, shares intelligence.

Supported by:
Threat Intelligence Analysts
Malware Analysts
Threat Hunters

Security Engineering & Architecture Team

Responsibilities:
Designs secure infrastructure, integrates security in DevSecOps and cloud environments.

Supported by:
Cloud Security Architect
DevSecOps Engineers
Network Security Engineers
Penetration Testers
Vulnerability Management Lead

Identity & Access Management (IAM) Team

Led by: IAM Manager
Responsibilities:
Manages access rights and identity systems, implements SSO, MFA.

Supported by:
IAM Engineers
Access Governance Analysts

Application Security Team
Led by: Application Security Manager

Responsibilities:
Integrates security into software development, conducts code reviews.

Supported by:
Application Security Engineers
Vulnerability Management Specialists

References

Force, J. T. (2017). Security and privacy controls for information systems and organisations (No. NIST Special Publication (SP) 800-53 Rev. 5 (Withdrawn)). National Institute of Standards and Technology.

Pascoe, C., Quinn, S. & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Papers (CSWP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.CSWP.29, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=957258

Ross, R. (2011). Managing Information Security Risk: Organization, Mission, and Information System View, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=908030

Vasquez, C. (2024, July 12). Phone and text message records of 'nearly all' AT&T customers stolen. CyberScoop. https://cyberscoop.com/att-data-breach-snowflake/#:~:text=%E2%80%9CEvery%20phone%20number%20you've,from%20privacy%20and%20security%20experts.

AT&T. (2024, July 12). AT&T Addresses Illegal Download of Customer Data. About.att.com. https://about.att.com/story/2024/addressing-illegal-download.html

JUST SOLUTIONS, INC. (2024, April 2). AT&T Data Breach: Cybersecurity Lessons for SMBs. https://www.linkedin.com/pulse/att-data-breach-cybersecurity-lessons-smbs-just-solutions-inc--lflfe/

Whited, R. (2024, July 19). The AT&T Data Breach and What Small Businesses Can Learn - ARF Financial. ARF Financial. https://www.arffinancial.com/the-att-data-breach-and-what-small-businesses-can-learn/

Lennon, Mike. “AT&T Data Breach: ‘Nearly All’ Wireless Customers Exposed in Massive Hack.” SecurityWeek, 19 July 2024, www.securityweek.com/att-data-breach-nearly-all-wireless-customers-exposed-in-massive-hack/

CrowdStrike, Inc. (2023). 2023 Cloud Risk Report. https://www.crowdstrike.com/cloud-risk-report/

Kurtz, G. & CrowdStrike. (2024). CROWDSTRIKE 2024 GLOBAL THREAT REPORT. https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

CROWDSTRIKE INCIDENT RESPONSE. (n.d.). https://go.crowdstrike.com/rs/281-OBQ-266/images/eBookCrowdStrikeIncidentResponse.pdf

Cichonski, P. , Millar, T. , Grance, T. and Scarfone, K. (2012), Computer Security Incident Handling Guide, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-61r2

IANS Faculty. (2021, February 14). *How to Choose the Right SOC Model*. IANS. Retrieved October 6, 2024, from https://www.iansresearch.com/resources/all-blogs/post/security-blog/2021/04/30/how-to-choose-the-right-soc-model

Kidd, C. (2023, November 14). *SOCs: Security Operation Centers Explained | Splunk*. Splunk. Retrieved October 6, 2024, from https://www.splunk.com/en_us/blog/learn/soc-security-operation-center.html

Staff, C. (2023, September 12). Security and privacy laws, regulations, and compliance: The complete guide. CSO Online. https://www.csoonline.com/article/570281/csos-ultimate-guide-to-security-and-privacy-laws-regulations-and-compliance.html

Alhajeid, A. (2024, February 23). *Navigating Key Cybersecurity Certifications for Your Business*. Wizard Cyber. https://wizardcyber.com/list-of-all-the-cyber-security-certifications-your-business-should-get/#:~:text=ISO%2027001%20Certification&text=It%20provides%20a%20framework%20for,to%20protect%20its%20information%20assets.

Sharma, S. (2024, April 19). Choosing SOC Tools? Read This First [2024 Guide]. D3 Security. https://d3security.com/blog/2024-guide-choosing-soc-tools/