



Information Security Program For CrowdStrike

Team Members:

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



FINAL PRESENTATION



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)
Degree of Dependency	Technology				People
	Process/Govern				

Asset Inventory

Hardware Inventory

Hardware categories	Department ownership
1. Mobile Phones & Sim Cards	Facilities Management
2. Servers	IT Department
3. IAM Devices	Security Department
4. Storage Devices	IT Department
5. Printers & Scanners	Facilities Management
6. Desktop Computers & Laptops	IT Department
7. Security Cameras	Security Department
8. Network Devices	IT Department
9. Projectors	Facilities Management
10. 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:

Physical Data

Log Data

Sensitive Data

Security Regulations and Certifications



Regulations:

- General Data Protection Regulation(GDPR)
- Federal Information Security Management Act (FISMA)
- California Consumer Privacy Act (CCPA)

Certifications:

- ISO 27001
- SOC 2

Incident Response Plan and SOC



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

Response Team Stakeholders

CSO/CISO, Incident response manager, Security operations Centre team, Threat Intelligence team, Forensic Team, PR team, Legal and compliance team, Third-party vendors, Law Enforcement, Regulatory Bodies, Law Firms

Reporting

C-suite, Clients/Customers, Employees/ teams, Insurance Carriers

Service Level Agreement(SLA)

Downtime- 5 hours, Detection time- 1 Day, Containment Time- 2 Day Attacker Dwell time- 2 Day, Recovery Time Objective- 6 hours, Recovery Point Objective -12 Hours

SOC Model

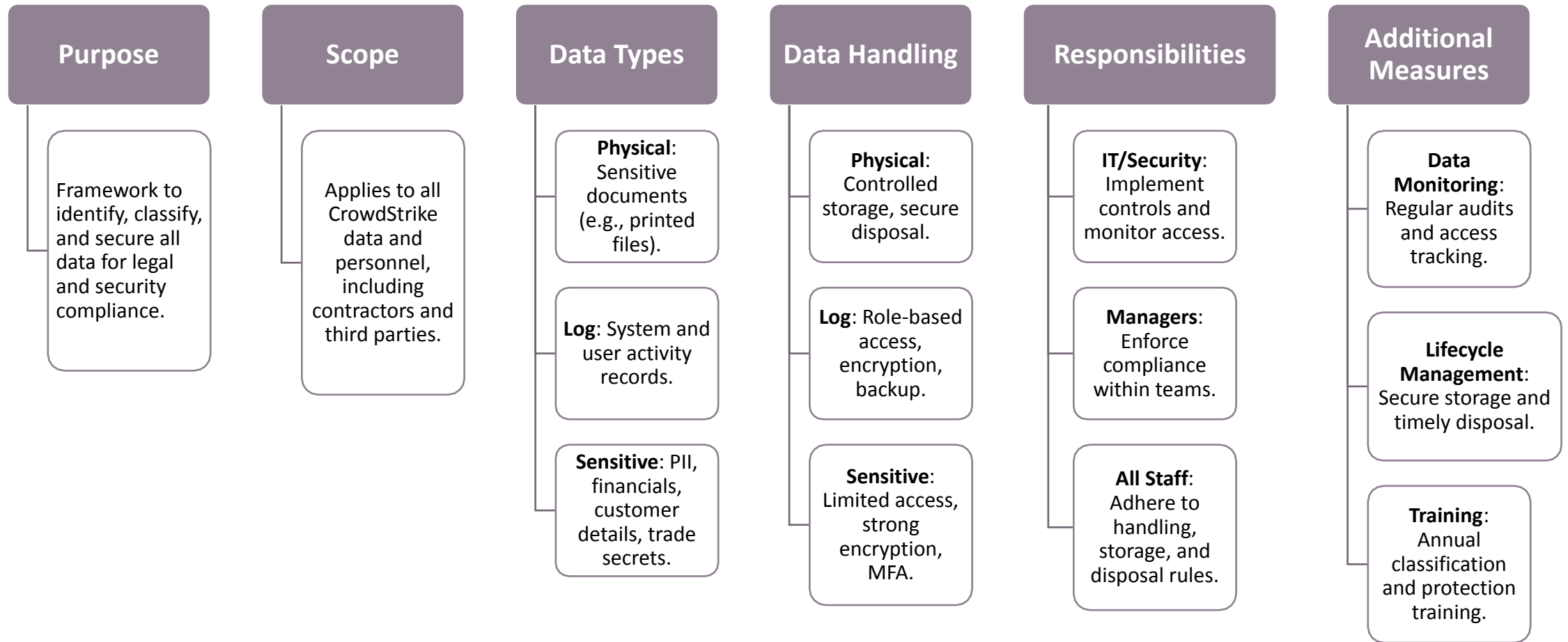
Internal/Dedicated SOC

Business Impact Analysis

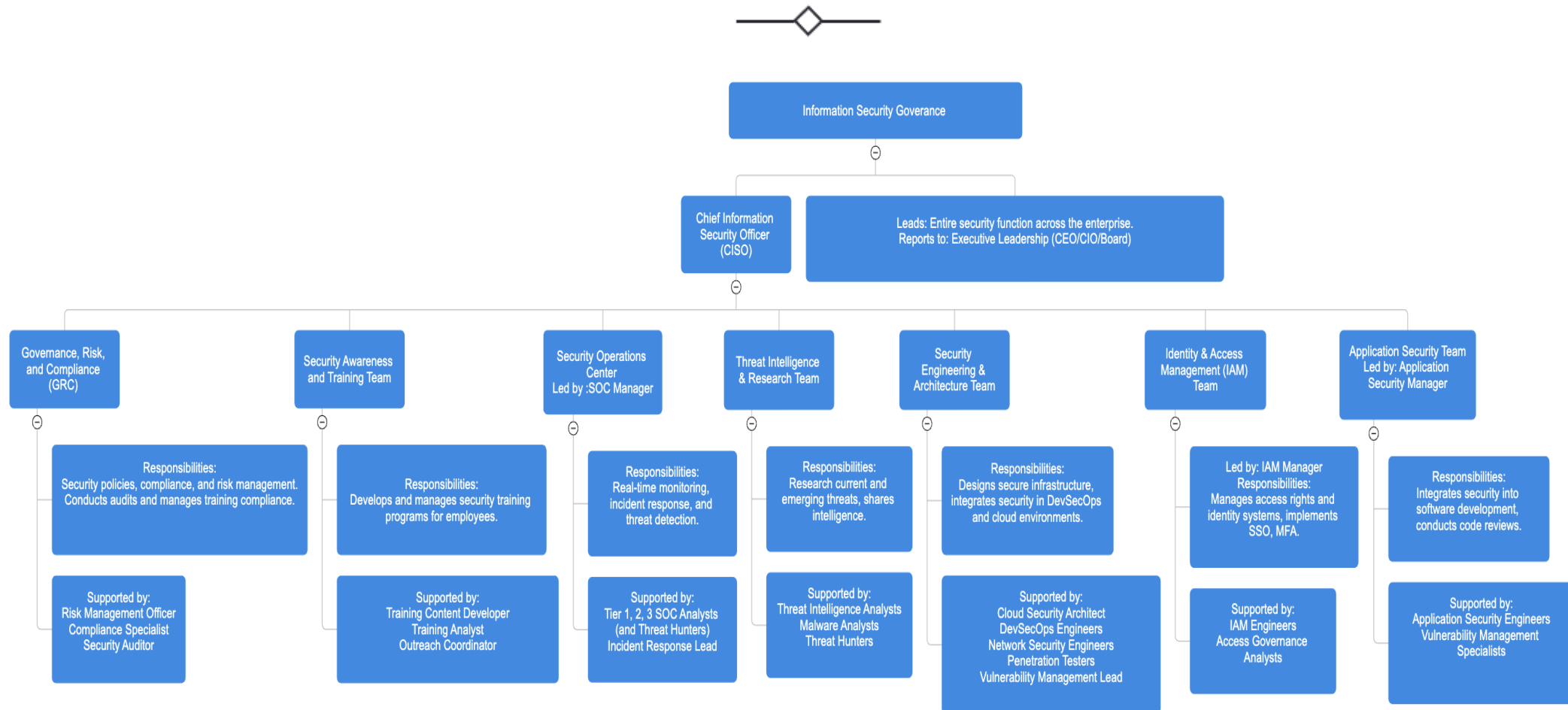


Application Name	Business Process	Financial Impact	Operational Impact	Recovery Objectives	Workaround Processes
<ul style="list-style-type: none">• ERP (Enterprise Resource Planning) System	<ul style="list-style-type: none">• Integrates and manages key Supply Chain, HR, Operations, and Finance processes.• Supports real-time data processing and inter-departmental communication.	<ul style="list-style-type: none">• Disruption may lead to lost revenue (up to \$500,000/day), payroll delays, and supply chain inefficiencies.	<ul style="list-style-type: none">• Reduced productivity and customer service due to lack of real-time information, affecting decision-making and satisfaction.	<ul style="list-style-type: none">• RTO: 4 hours• RPO: 12 hour	<ul style="list-style-type: none">• Use Excel for basic Inventory/Financial tracking and cloud Backup/Email for communication until recovery.

Data Classification Policy



Security Team Organizational Structure



THANK YOU

