Information Security Program For CrowdStrike

Team Members:

1. Harika Aakula
2. Karthik Reddy Guntakandla
3. Madhusudan Kummari
4. Sai Nikhil Reddy Kura
5. Namo Bhavani Maganti
6. Dhanesh Reddy Pulagam
7. Harshith Shivaswamy

Mid Term Presentation

MISSION, VISION AND GOALS

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

1. Ensure compliance with security frameworks.
2. Protecting CrowdStrike reputation
3. Monitoring and responding to the threats across the entire company network

STRATEGIC OBJECTIVES, OUTCOMES AND INITIATIVES

Strategic Objective	Outcomes	Strategic Initiatives
Enhance Threat intelligence and response capabilities	• Enhanced accuracy of threat detection • Improved Incident response • Time to detect and time to respond potentially reduces	Investing in advanced threat intelligence
Boost cloud security posture and robustness	• Potential decrease in risk of cloud breaches • Enhanced visibility into cloud activity • Improved compliance of cloud security standards with frameworks	Adopt Zero trust approach and Implement Cloud-native security control
Enhance Identity and Access Management Security	• Minimal Lateral Moment • Improved protection against Credential theft • Reduction in phishing and social engineering attacks	Implementing Strong MFA and Educating employees

SECURITY FRAMEWORK

Control Framework-
NIST 800-53

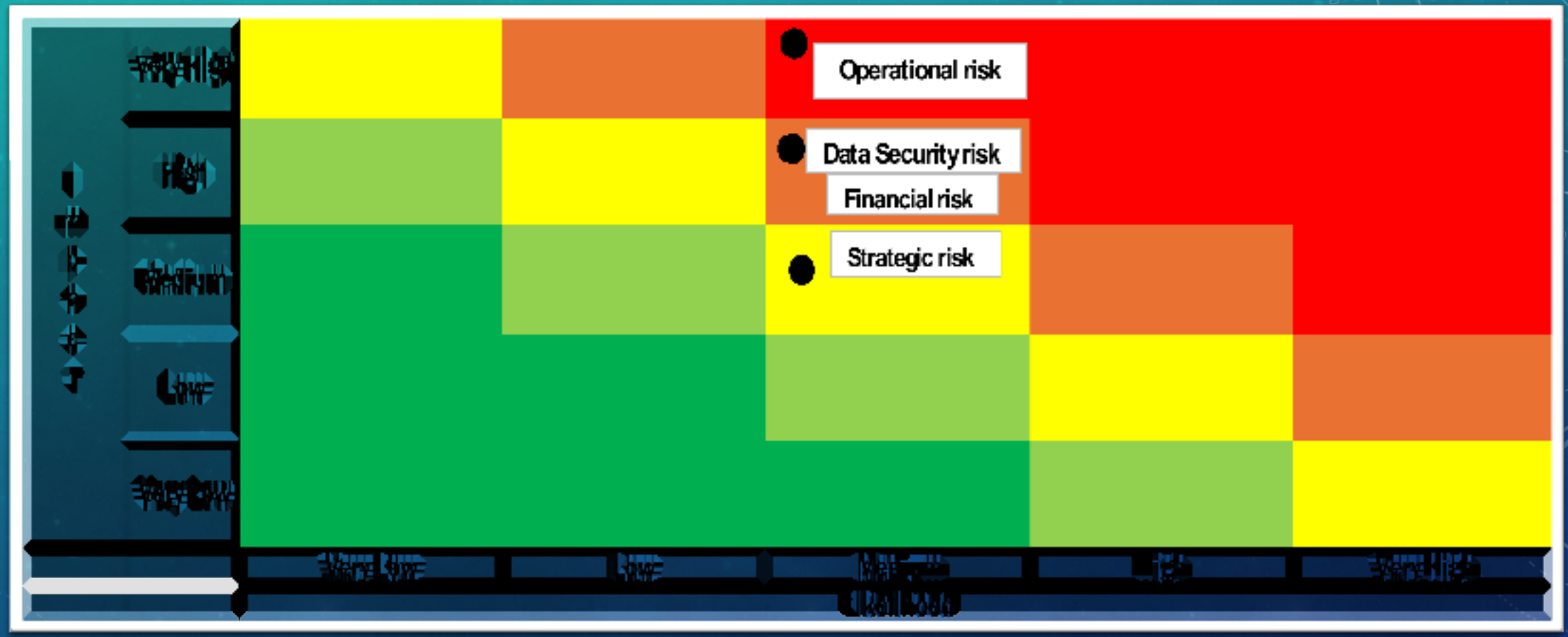
Program Framework-
NIST CSF

Risk Framework-
NIST 800-39

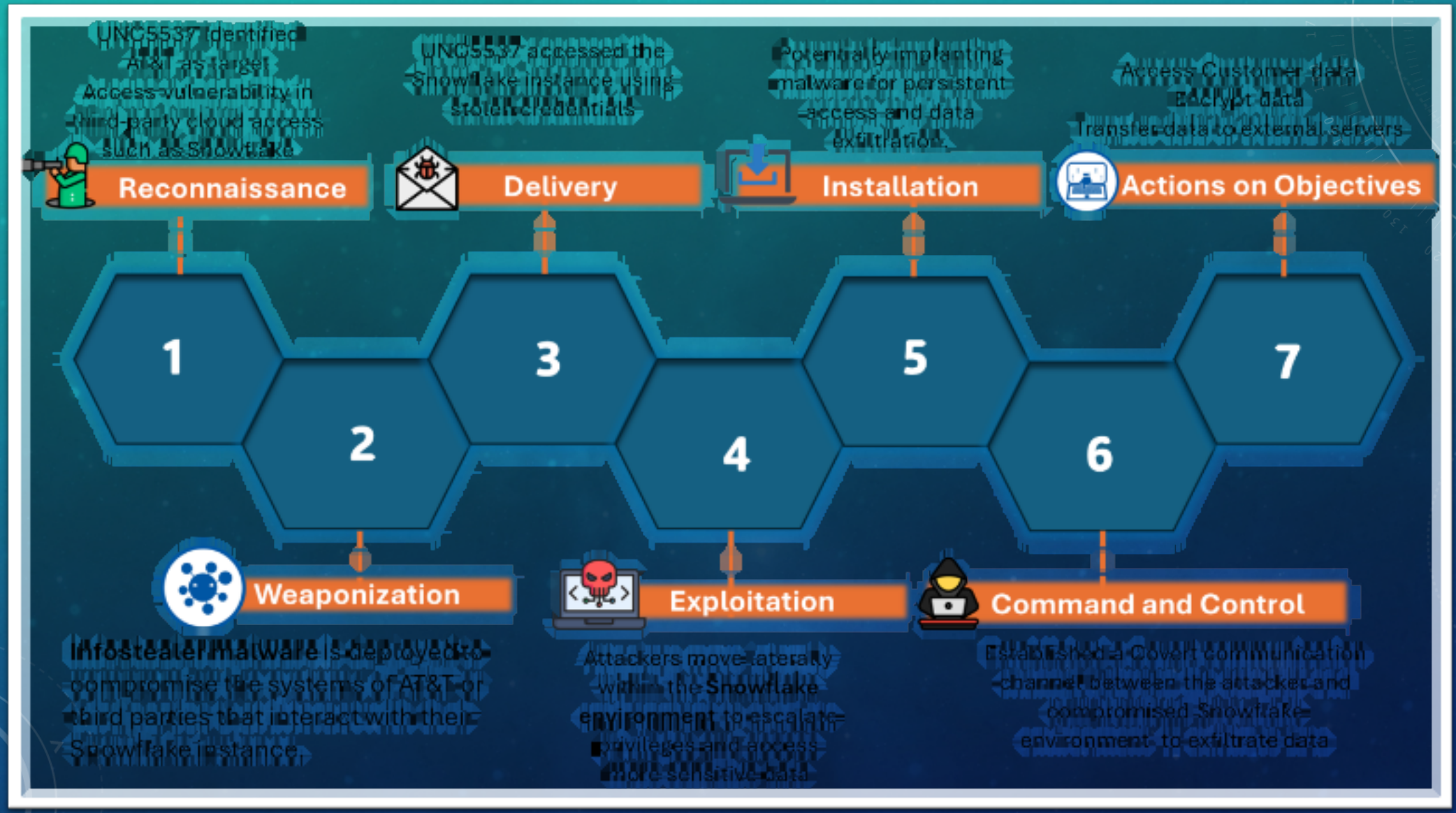
RISK APPETITE STATEMENT

Risk Name	Risk Appetite Statement
Data Security Risk	CrowdStrike has no tolerance towards data breaches, especially breaches which involve unauthorized access or 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
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.
Operational Risk	CrowdStrike has a low tolerance for operational disruptions, as incidents such as cloud security misconfigurations can lead to service interruption and downtime. Our organization is aimed toward maintaining operational resilience in growing cloud complexities
Financial Risk	CrowdStrike has little tolerance for financial risk as the company recognizes that robust cyber security measures come at a considerable price. Moreover, organizations seek to minimize financial exposure for incidents like cyberattacks through vital prevention and detection mechanisms

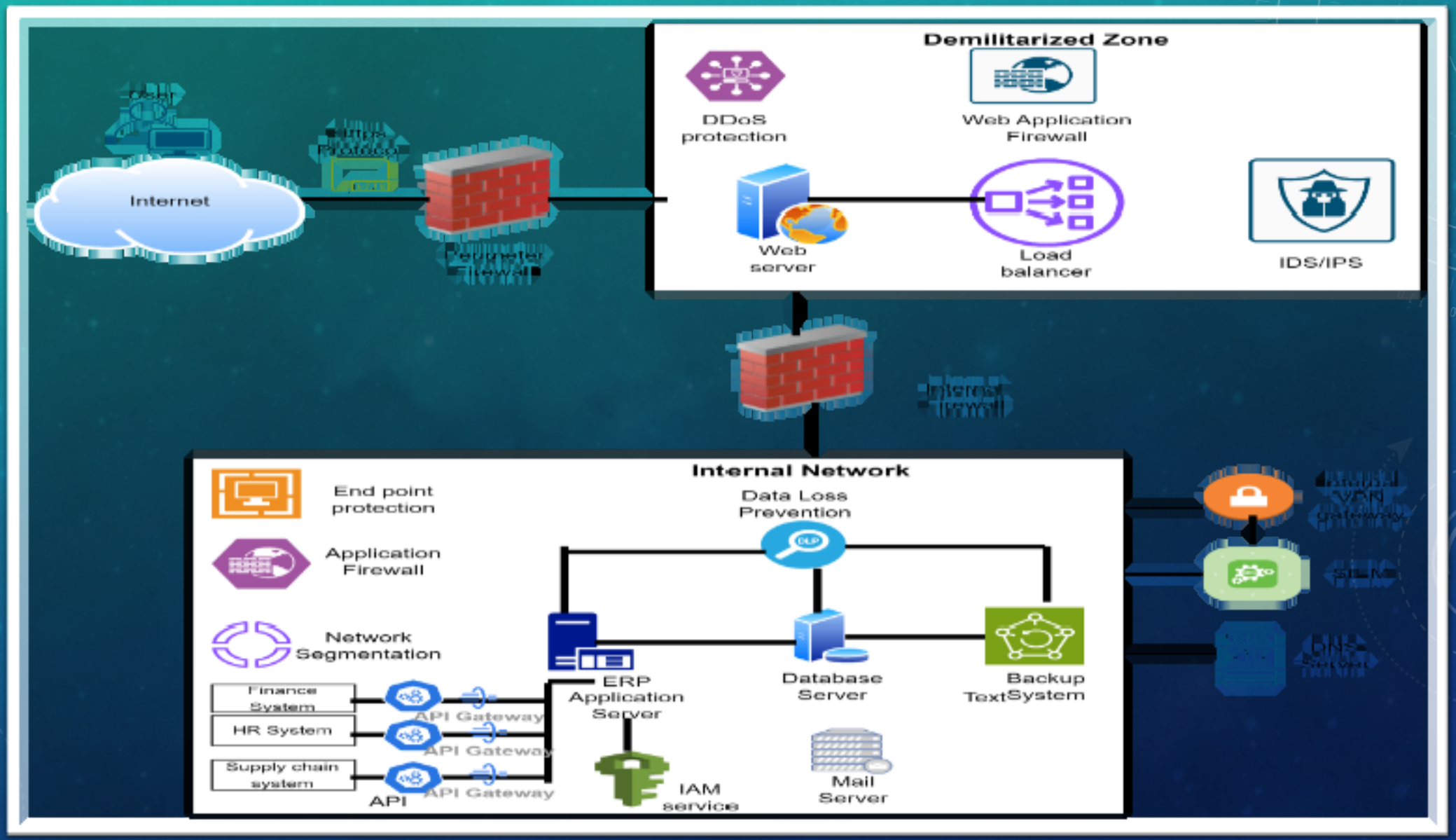
HEAT MAP & PRIORITIZATION



SECURITY INCIDENT MAPPING



SECURE ARCHITECTURAL DESIGN



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)	N/A
Applications	Checkmarx (SAST,DAST, SW Asset Mgt, Fuzzers)	Imperva (RASP, WAF)	N/A	N/A	N/A
Networks	Qualys (Netflow, Network vuln Scanner)	Palo Alto Netwoks Cisco ASA Firewall (FW, IPS/IDS)	Cloudfare (DDoS Detection)	Cloudfare (DDoS Response, NW Forensics)	N/A
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)	N/A	N/A

Degree of Dependency

People

Technology

Process/Govern

THANK YOU