One Platform. 34 Controls. ACSC-Aligned Architecture.

Mapping Cisco Security to ACSC Top 37 and NIST CSF 2.0

JJ Jones, Cisco Solutions Engineering Leader

Contents

Executive Summary

Australian organisations face a compliance landscape where Essential Eight is mandated, NIST Cybersecurity Framework (CSF) 2.0 is best practice, and both frameworks are treated as separate exercises. This whitepaper eliminates that duplication.

Cisco Security delivers 34 of 37 Australian Cyber Security Centre (ACSC) Top 37 mitigation strategies through unified architecture — including all 8 Essential Eight controls. By architecting to NIST CSF 2.0, organisations can demonstrate Essential Eight alignment through their existing security architecture.

This mapping enables three outcomes: (1) streamlined compliance assessments with line-by-line ACSC capability coverage documentation, (2) clear maturity level pathways tied to deployment patterns, and (3) competitive differentiation against point-solution aggregation through network-native segmentation and Splunk-powered detection.

1. Introduction

Australian CISOs face a structural problem: Essential Eight is compliance-mandated, NIST CSF 2.0 is the board-level strategic framework, and most organisations treat them as separate implementations. This creates vendor sprawl, duplicated effort, and attribution blind spots.

Cisco's approach resolves this by aligning portfolio architecture to NIST CSF 2.0 functions — providing Essential Eight capability coverage as a derivative outcome. The result: one platform, 34 of 37 ACSC strategies addressed, and measurable control effectiveness without point-solution aggregation.

The NIST CSF 2.0 provides a unique value proposition compared to other frameworks such as ISO 27001, CIS Controls, or Australia's Essential Eight. While most frameworks offer a "checklist" of security controls, NIST CSF serves as a strategic communication tool that bridges the gap between technical teams and executive leadership.

The primary value of NIST CSF lies in its **outcome-based approach**. Rather than mandating specific technologies, the framework focuses on six high-level functions: **Govern, Identify, Protect, Detect, Respond, and Recover**.

- **Common Language:** It provides a non-technical vocabulary that allows Chief Information Security Officers (CISOs) and cybersecurity leadership teams to explain cybersecurity risks and investments to Board members and stakeholders.
- **Flexibility and Scalability:** It is designed to be tailored. Australian organisations can adapt the framework to meet local Australian requirements (such as APRA CPS 234) while maintaining a global standard.
- **Risk-Based, Not Compliance-Based:** Unlike "pass/fail" frameworks, NIST CSF uses "Implementation Tiers" (Partial to Adaptive) to help organisations measure their maturity and prioritise spending based on their specific risk appetite.

Most mature organisations do not choose just one framework; they use NIST CSF as the "umbrella" and map other frameworks under it.

Feature	NIST CSF 2.0	ISO/IEC 27001:2022	CIS Controls (v8.1)	Essential Eight (AU)
Primary Goal	Risk Management and Strategy	Global Certification and Trust	Technical "Cyber Hygiene"	Targeted Threat Mitigation
Focus	• Strategic • Business	• Governance • Process	• Technical • Operational	• Tactical • Baseline
Certification	No (Self-assessment)	Yes (External Audit)	No	No (Maturity Levels)
Best For	Communicating risk to the Board and aligning security with business goals.	Proving security posture to international clients and partners.	Technical teams needing a prioritized "to-do" list of controls.	Australian organisations seeking a baseline against common local threats.

The Australian Signals Directorate (ASD) Strategies to Mitigate Cybersecurity Incidents are a prioritised list of mitigation strategies that provide a comprehensive, defence-in-depth framework to assist organisations mitigate cybersecurity incidents that could be caused by various cyber threats. The strategies offer a holistic approach to cybersecurity encompassing a wide range of technical and administrative controls. The effectiveness of implementing a control is classified as "Essential", "Excellent", "Very Good", "Good", and "Limited". There are eight controls classed as Essential which are the **Essential Eight** that are a prioritised set of baseline mitigation strategies designed to help organisations protect their internet-connected information technology environments from various cyber threats.

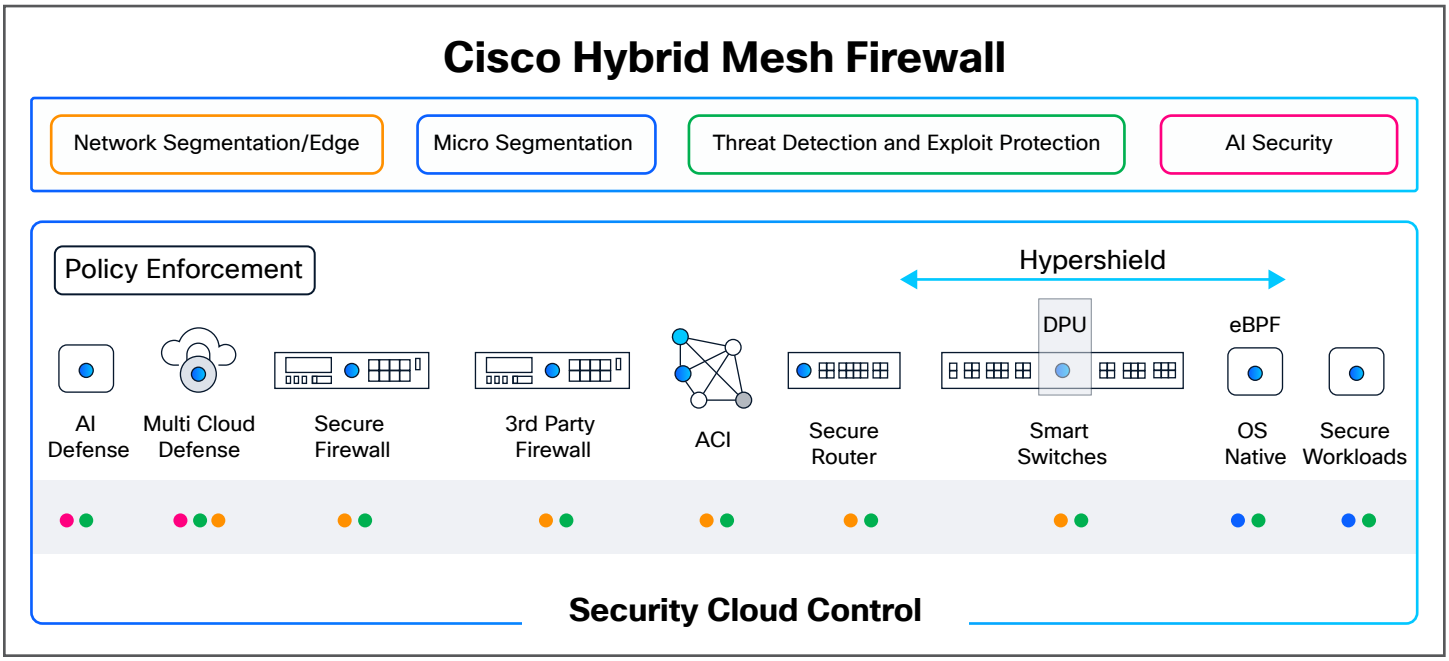
As depicted in the Cisco Security Portfolio, Splunk, and The NIST Cybersecurity Framework 2.0 solution guide, Cisco® aligns its security architecture directly with the NIST CSF functions to help organisations move from "theory" to "implementation." For example:

- **Identify and Govern:** Cisco **Identity Services Engine (ISE)** helps organisations identify every device on the network, fulfilling the "Asset Management" category of the Identify function.
- **Protect:** Cisco **Secure Access, a Security Service Edge (SSE)** solution, and Duo provide the Zero Trust foundations required for the Protect function.
- **Detect and Respond:** Cisco **Secure Cloud Analytics** and **Talos®** threat intelligence provide the continuous monitoring and rapid response capabilities central to the Detect and Respond functions.
- **Interoperability:** Cisco solutions are designed to be "open," meaning they can report data into a NIST CSF–aligned dashboard even if you are also using ISO 27001 for compliance.

The purpose of this paper is to inform and educate by mapping Cisco security portfolio capabilities across NIST CSF 2.0 and the Australian Cybersecurity Centre (ACSC) Top37 Strategies to Mitigate Cybersecurity Incidents of which the Essential Eight are a subset list. The Top37 provide more holistic defence in-depth mitigations over and above a baseline such as the Essential Eight.

Cisco Security

Hybrid Mesh Firewall

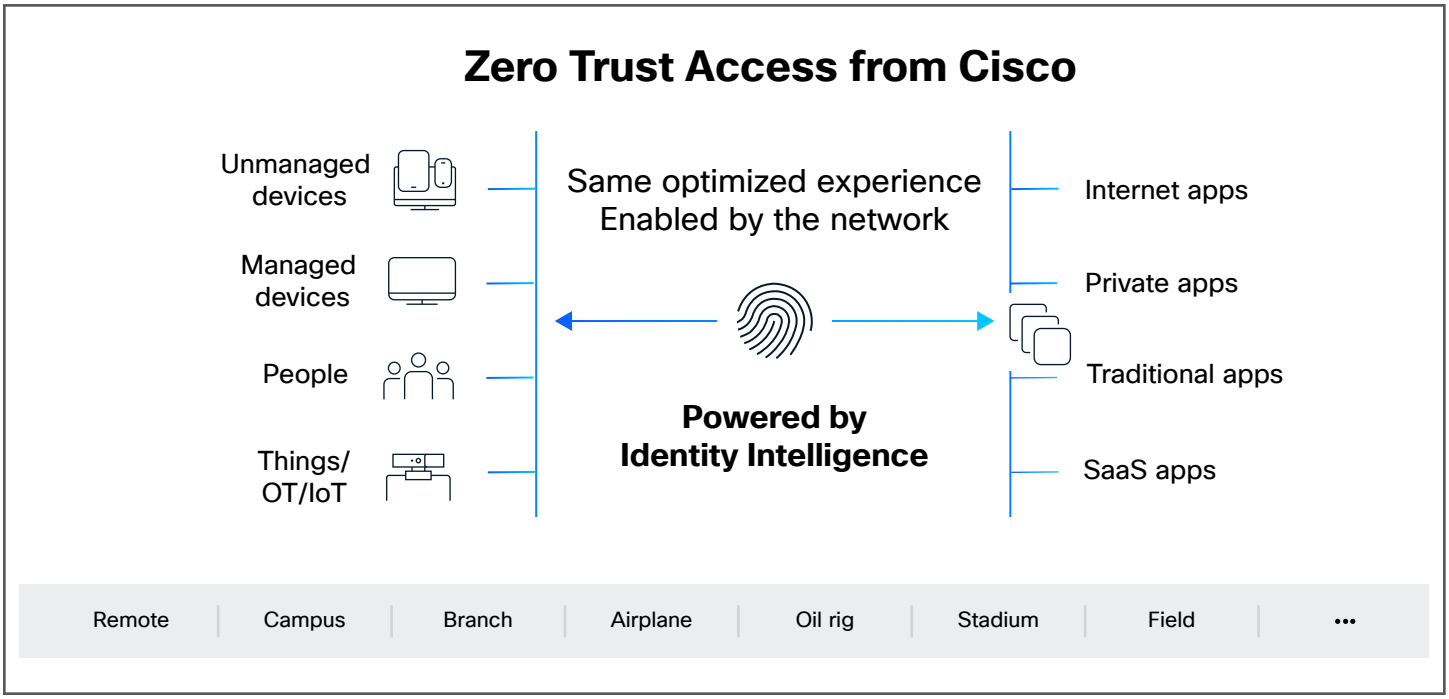


The Cisco Hybrid Mesh Firewall solution is a highly distributed security fabric optimised to stop advanced threats, protect application vulnerabilities, and implement zero trust segmentation across environments, fusing security into the network, cloud, container, and workload for a highly distributed fabric.

Cisco's Hybrid Mesh Firewall offers:

- **Intelligent Centralised Management:** Automatically configures, deploys, and auto scales firewalls across multi-cloud environments without scripting. Plus, the AI Assistant reduces management overhead and frees up resources and expertise.
- **Advanced Threat Protection:** Sees through encryption to detect threats in encrypted traffic without sacrificing performance using industry's first, ML-based encrypted visibility engine. Where decryption is essential, high performance hardware offload architecture delivers price-performance leadership and deep visibility. Protect against known and unknown threats with Cisco Talos Threat Intelligence, industry-leading Snort 3 IPS, and Snort ML.
- **Segmentation:** Prevent unauthorized lateral movement and safeguard applications across data centre and clouds with topology-aware security that understands app dependencies and applies zero-trust segmentation policies across the Cisco security fabric.
- **AI Model Protection:** Fuses AI guardrails into the fabric of the network to safeguard in real-time against the dynamic threats introduced through the development and deployment of AI applications.
- **Exploit Protection:** Mitigates vulnerabilities by applying a surgical mitigation shield that is optimally placed in the path of the application to block the exploit–all while ensuring application uptime.

Zero Trust Access

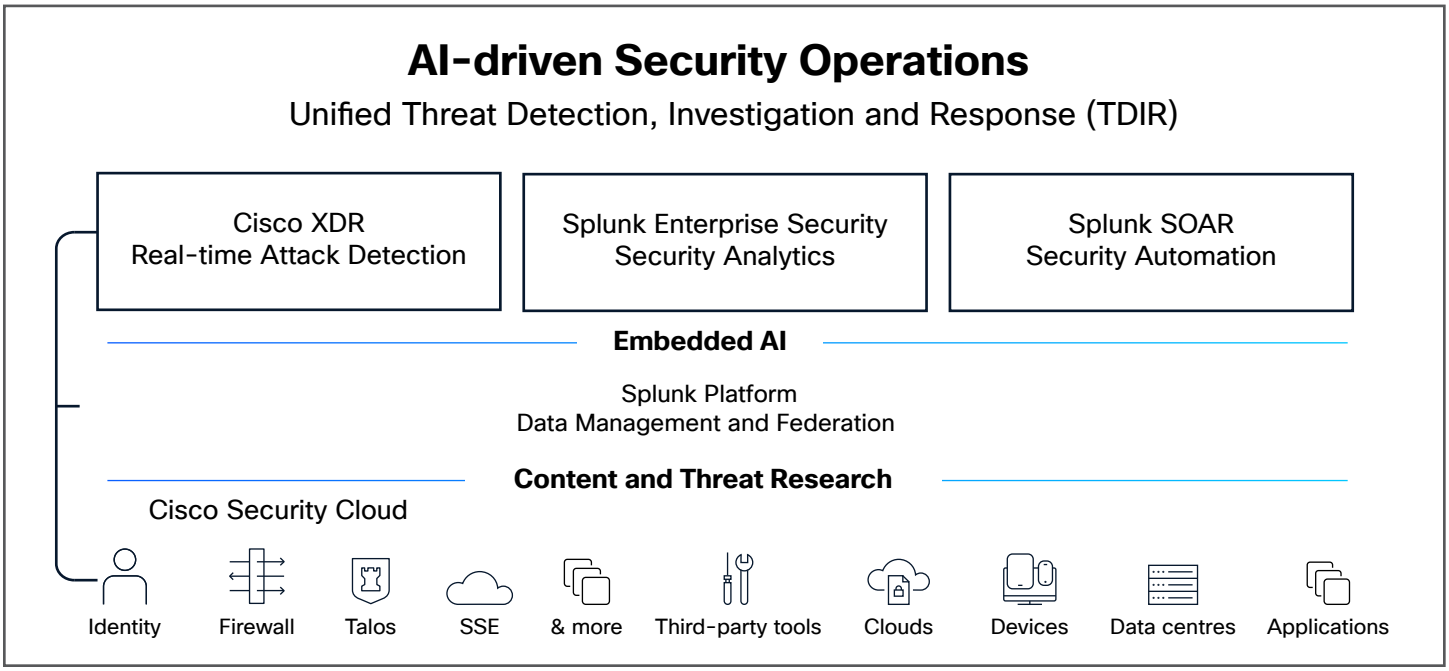


Zero Trust Access from Cisco is a comprehensive solution enabling every user and device to securely connect to any application, anywhere, ensuring a consistent experience. It unifies identity-first zero trust access for modern and legacy apps, IoT/OT devices, and complex network environments, combining industry-leading performance, policy assurance, and end-to-end visibility to eliminate complexity and protect critical assets. Cisco Zero Trust Access supports flexible enforcement, in the cloud or on-premises, so that sensitive data is protected, and governance objectives met. Our approach helps organisations **modernize application access** with Zero Trust Network Access (ZTNA) and VPN-as-a-Service in a consistent way, **extend identity context** to include users and things, and **build operational resilience** through end-to-end digital experience monitoring and policy assurance.

Cisco Zero Trust Access benefits include:

- **Networking expertise:** Foundational skills in SD-WAN, VPN, and firewalls ensure seamless zero-trust policy integration across hybrid environments.
- **Hybrid private access:** Consistent zero-trust policy enforcement for remote, branch, and campus users across cloud and on-premises environments from a single management tool.
- **Shadow AI management:** Detects and manages unauthorized AI applications to prevent data leakage and ensure compliance.
- **Comprehensive application support:** Seamless handling of modern, legacy, SaaS, and private apps without disruptions.
- **Dynamic risk-based access:** Continuously adjusts access based on user behaviour, device posture, and network conditions.

Security Operations – SOC of the Future



Cisco's vision for the Security Operations Center (SOC) of the future is an environment where security operations are not just reactive, but proactive–a world where threats are anticipated and neutralised before they have a devastating impact on an organisation. The SOC then becomes a powerful enabler to help an organisation strengthen its digital resilience. The SOC of the future is not just a concept; it is a reality built on innovation, powered by AI, and supported by continuous research. It's a world where security is proactive, intelligent, and automated, providing peace of mind in an ever-evolving threat landscape.

Cisco's SOC of the future includes several important elements:

- Cisco's **market-leading Splunk** Security Information and Event Management (SIEM) and innovative Cisco Extended Detection and Response (XDR) technologies are the foundation.
- **Federated data management** is at the heart of the transformation to achieve the SOC of the future where a vast network of data sources is seamlessly integrated and managed, providing a unified view of your security landscape ensuring that no threat goes unnoticed, no matter where it originates.
- **Advanced detections** are powered by cutting-edge algorithms that evolve with the threat landscape, ensuring defences are always one step ahead.
- **AI-accelerated** investigations bring the power of Artificial Intelligence (AI) to your fingertips with AI acting as your trusted advisor, rapidly sifting through vast amounts of data, pinpointing the root cause of incidents, and providing actionable insights.
- **Automated threat response** mechanisms act like a well-oiled machine, executing predefined actions to mitigate threats swiftly and effectively, ensuring that the SOC team can focus on strategic tasks, knowing that routine responses are handled automatically.
- **Embedded AI**, which acts as the engine driving the SOC of the future, supercharges all the above capabilities and ensures they work together harmoniously, creating a cohesive and robust security posture.
- A wealth of content and **threat intelligence research** supports this advanced infrastructure providing a library of the latest threat intelligence, curated by experts who are constantly monitoring the cyber landscape. This research informs and enhances every aspect of the SOC, ensuring you are always prepared for the next threat.

2. Detailed Mapping

Methodology

The mapping follows three layers:

1. **ACSC Strategy → NIST CSF 2.0 Function/Category:** Based on the primary security outcome of each ACSC strategy and aligned to the CSF Core taxonomy.
2. **NIST CSF 2.0 Category → Cisco Capability:** Based on Cisco's published CSF 2.0 portfolio mapping.
3. **Cross-validation:** Ensuring the Cisco capability is relevant in addressing the intent of the ACSC strategy.

Note: Some ACSC strategies span multiple NIST CSF categories. In such cases, the primary category is indicated with secondary mappings noted. Mappings are based on conceptual alignment consistent with NIST IR 8477[2] methodology.

Mapping Tables

1. Mitigation Strategies to Prevent Malware Delivery and Execution

1.1 Application Control (Essential)

ACSC Description: Prevent execution of unapproved/malicious programs including .exe, Dynamic Link Library (DLL), scripts (PowerShell, HTML Application [HTA]) and installers.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.PS (Platform Security)** – PR.PS-01 (Configuration management) – PR.PS-05 (Prevent unauthorised software execution)
Secondary NIST CSF 2.0	▪ PR.AA (Access Control) ▪ DE.CM (Continuous Monitoring)
Cisco Capabilities	▪ **Cisco Secure Endpoint** – Application control and execution prevention ▪ **Cisco Secure Firewall** – Network-layer enforcement ▪ **Cisco Secure Client** – Endpoint policy enforcement ▪ **Cisco Secure Access** – DNS and Web - layer blocking of malicious execution Pathways ▪ **Cisco Secure Email** – Preventing Malicious programs delivered via email

1.2 Patch Applications (Essential)

ACSC Description: Patch Flash, browsers, Office, Java, PDF viewers. Mitigate “extreme risk” vulnerabilities within 48 hours.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **ID.RA (Risk Assessment)** - ID.RA-01 (Vulnerability identification) - ID.RA-05 (Risk prioritisation)
Secondary NIST CSF 2.0	▪ PR.PS-02 (Software maintained commensurate with risk)
Cisco Capabilities	▪ **Cisco Secure Endpoint** – Endpoint vulnerability visibility ▪ **Cisco Secure Access** – Vulnerability prioritisation and patch tracking ▪ **Cisco Secure Workload** – Vulnerability prioritisation and patch tracking ▪ **Cisco Secure Network Analytics** – Detect behavioural anomalies ▪ **Splunk Exposure Analytics** – Asset inventory and vulnerability correlation

1.3 Configure Microsoft Office Macro Settings (Essential)

ACSC Description: Block macros from the internet; only allow vetted macros in trusted locations or digitally signed.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.PS (Platform Security)** - PR.PS-01 (Configuration management practices) - PR.PS-05 (Prevent unauthorised software execution)
Secondary NIST CSF 2.0	▪ PR.DS (Data Security)
Cisco Capabilities	▪ **Cisco Secure Endpoint** – Malicious macro detection and blocking ▪ **Cisco Secure Email** – Attachment analysis and macro quarantine ▪ **Cisco Secure Access** – Block access to malicious or unwanted domains (bad domains) and to inspect and block harmful files ▪ **Splunk Enterprise Security** – Microsoft office macro execution event logging, detection, and alerting through correlation searches and endpoint telemetry

1.4 User Application Hardening (Essential)

ACSC Description: Block Flash, ads, Java in browsers; disable unneeded features in Office and PDF viewers.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.PS (Platform Security)** – PR.PS-01 – PR.PS-02 – PR.PS-03
Secondary NIST CSF 2.0	▪ PR.IR (Technology Infrastructure Resilience)
Cisco Capabilities	▪ **Cisco Duo Identity and Access Management (IAM)** – Identifying and blocking access from endpoints using vulnerable or unauthorized plugins like Flash and Java ▪ **Cisco Secure Client** – Endpoint compliance and hardening posture ▪ **Cisco Secure Endpoint** – Threat prevention on hardened endpoints ▪ **Cisco Secure Access** – Blocking malicious web content including ads and malvertising

1.5 Automated Dynamic Analysis/Sandboxing (Excellent)

ACSC Description: Analyse email and web content in a sandbox; block if suspicious behaviour is identified.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **DE.CM (Continuous Monitoring)** – DE.CM-09 (Computing hardware, software, and data monitored) ▪ **DE.AE (Adverse Event Analysis)** – DE.AE-02
Secondary NIST CSF 2.0	▪ PR.DS (Data Security)
Cisco Capabilities	▪ **Cisco Secure Malware Analytics** – Dynamic sandboxing of files and URLs ▪ **Cisco Secure Email** – Sandboxed email attachment analysis ▪ **Cisco Secure Endpoint** – Behavioural analysis and retrospective detection ▪ **Cisco Secure Access** ▪ **Cisco Secure Web Appliance**

1.6 Email Content Filtering (Excellent)

ACSC Description: Allow only approved attachment types; analyse/sanitise hyperlinks and Office/PDF attachments; quarantine macros.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.DS (Data Security)** – PR.DS-02 (Data-in-transit protection) ▪ **PR.PS** – PR.PS-05
Secondary NIST CSF 2.0	▪ DE.CM-01
Cisco Capabilities	▪ **Cisco Secure Email** – Advanced email filtering, attachment scanning, URL rewriting

1.7 Web Content Filtering (Excellent)

ACSC Description: Allow only approved web content types and reputable sites; block malicious domains, IPs, anonymity networks, and free domains.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.PS (Platform Security)** – PR.PS-05 ▪ **DE.CM** – DE.CM-01
Secondary NIST CSF 2.0	▪ PR.IR-01
Cisco Capabilities	▪ **Cisco Secure Access** – DNS-layer web filtering, threat intelligence-driven domain blocking ▪ **Cisco Secure Firewall** – URL filtering and reputation-based blocking ▪ **Cisco Meraki™ MX** – URL filtering and reputation-based blocking ▪ **Cisco Secure Web Appliance** – Proxy-based web content inspection

1.8 Deny Direct Internet Connectivity/Gateway Firewall (Excellent)

ACSC Description: Require use of authenticated proxy, split DNS, and email gateway for outbound connections.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.IR (Technology Infrastructure Resilience)** – PR.IR-01 (Networks protected from unauthorised access) ▪ **PR.PS** – PR.PS-01
Secondary NIST CSF 2.0	▪ DE.CM-01
Cisco Capabilities	▪ **Cisco Secure Firewall** – Perimeter enforcement and outbound traffic control ▪ **Cisco Meraki MX** – Perimeter enforcement and outbound traffic control ▪ **Cisco Secure Access** – Zero trust secure internet access controls

1.9 Operating System Exploit Mitigation (Excellent)

ACSC Description: Enable OS-level exploit mitigations including Data Execution Prevention (DEP) and Address Space Layout Randomisation (ASLR).

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.PS (Platform Security)** – PR.PS-01 – PR.PS-03 (Hardware maintained commensurate with risk)
Secondary NIST CSF 2.0	▪ PR.IR-03
Cisco Capabilities	▪ **Cisco Secure Endpoint** – Exploit prevention capabilities at the endpoint layer ▪ **Cisco XDR (Forensic)** – Provides visibility into the OS stack for detections ▪ **Splunk Enterprise Security** – Detection and alerting of exploit mitigation bypass attempts and exploitation activity using endpoint telemetry

1.10 Server Application Hardening (Very Good)

ACSC Description: Harden internet-accessible web applications and databases; sanitise input, use Transport Layer Security (TLS).

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.PS (Platform Security)** - PR.PS-01 - PR.PS-06 (Secure software development) ▪ **PR.DS** - PR.DS-02
Secondary NIST CSF 2.0	▪ PR.IR-01
Cisco Capabilities	▪ **Cisco Secure Web Application Firewall (WAF)** – Web application input validation and attack blocking ▪ **Cisco Secure Firewall** – Server traffic inspection ▪ **Cisco Multicloud Defense** – Cloud workload protection ▪ **Cisco Secure Workload** – Workload protection founded on least-privilege access ▪ **Isovalent** - Container-based protections founded on least-privilege access

1.11 Operating System Hardening (Very Good)

ACSC Description: Harden OSes and network devices; disable Remote Desktop Protocol (RDP), AutoRun, LanMan, Server Message Block/Network Basic Input/Output System [SMB/NetBIOS], Link-Local Multicast Name Resolution (LLMNR), Web Proxy Auto-Discovery (WPAD).

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.PS (Platform Security)** - PR.PS-01 - PR.PS-03
Secondary NIST CSF 2.0	▪ PR.IR-01 ▪ ID.AM
Cisco Capabilities	▪ **Cisco Secure Endpoint** – OS-level threat prevention ▪ **Cisco Meraki Systems Manager** – Device configuration baseline enforcement ▪ **Splunk Enterprise Security** – Continuously monitoring system configuration changes, detecting drift from secure baselines, and alerting on misconfigurations or privilege abuse to support ACSC Essential Eight compliance

1.12 Antivirus with Heuristics and Reputation Ratings (Very Good)

ACSC Description: Use AV with heuristics and reputation to check file prevalence and digital signatures.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **DE.CM (Continuous Monitoring)** – DE.CM-09 ▪ **PR.PS (Platform Security)** – PR.PS-05
Secondary NIST CSF 2.0	· DE.AE-02
Cisco Capabilities	▪ **Cisco Secure Endpoint** – Heuristic and reputation-based malware prevention ▪ **Cisco Secure Access** – Reputation-based blocking at the DNS and web layer

1.13 Control Removable Storage Media (Very Good)

ACSC Description: Block unapproved USB, CD/DVD, smartphones, tablets, and wireless devices.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.PS (Platform Security)** – PR.PS-01 – PR.PS-05 ▪ **PR.DS (Data Security)** – PR.DS-01 (Data-at-rest protection)
Secondary NIST CSF 2.0	· PR.AA-06
Cisco Capabilities	▪ **Cisco Secure Access** – Block unauthorised smartphones, tablets, wireless devices for application access ▪ **Cisco Duo IAM** – Block unauthorised smartphones, tablets, wireless devices for application access ▪ **Cisco Secure Endpoint** – Device control and USB blocking ▪ **Cisco Identity Services Engine (ISE)** – Device profiling and network access control for connected endpoints ▪ **Cisco Secure Client** – Endpoint Data Loss Prevention (DLP)

1.14 Block Spoofed Emails (SPF, DMARC) (Very Good)

ACSC Description: Configure Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting, and Conformance (DMARC) DNS records to mitigate email spoofing.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.DS (Data Security)** – PR.DS-02 ▪ **PR.PS (Platform Security)** – PR.PS-01
Secondary NIST CSF 2.0	▪ DE.CM-01
Cisco Capabilities	▪ **Cisco Secure Email** – SPF, DomainKeys Identified Mail (DKIM), DMARC enforcement and email authentication

1.15 User Education (Phishing Awareness) (Good)

ACSC Description: Educate users on phishing, weak passphrases, passphrase reuse, and unapproved services.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.AT (Awareness and Training)** – PR.AT-01 – PR.AT-02
Secondary NIST CSF 2.0	▪ GV.RR-04
Cisco Capabilities	▪ **Cisco Secure Email and KnowB4 Security Coach** ▪ **Cisco Secure Access and KnowB4 Security Coach** ▪ **Cisco Duo** – MFA enforcement as a technical complement to user education

2. Mitigation Strategies to Limit the Extent of Cybersecurity Incidents

2.1 Restrict Administrative Privileges (Essential)

ACSC Description: Limit admin privileges based on user duties; revalidate regularly; no privileged use for email/web browsing.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.AA (Identity Management, Authentication, and Access Control)** – PR.AA-05 (Least privilege and separation of duties) – PR.AA-01
Secondary NIST CSF 2.0	▪ PR.PS-01
Cisco Capabilities	▪ **Cisco Duo** – Privileged access enforcement and Multifactor Authentication (MFA) ▪ **Cisco Secure Access** – Zero Trust Network Access (ZTNA) ▪ **Cisco Identity Services Engine (ISE)** – Role-based access control ▪ **Splunk Enterprise Security** – Privileged access monitoring and policy enforcement validation ▪ **Splunk User Entity Behaviour Analytics** – Detect anomalous or high-risk privileged account activity

2.2 Patch Operating Systems (Essential)

ACSC Description: Patch OSes and network devices with “extreme risk” vulnerabilities within 48 hours; use latest supported OS versions.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **ID.RA (Risk Assessment)** – ID.RA-01 – ID.RA-05 ▪ **PR.PS (Platform Security)** – PR.PS-02 – PR.PS-03
Secondary NIST CSF 2.0	▪ ID.AM-08

Mapping Layer	Detail
Cisco Capabilities	▪ **Cisco Secure Workload** – OS-level vulnerability tracking, prioritisation, and virtual patching ▪ **Cisco Hypershield** – OS-level vulnerability virtual patching ▪ **Cisco Secure Firewall** – Integration with vulnerability scanners and virtual patching ▪ **Splunk Exposure Analytics** – Patch gap identification across asset inventory

2.3 Multi-Factor Authentication (Essential)

ACSC Description: MFA for VPNs, RDP, SSH, remote access, and privileged actions or access to important data repositories.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.AA (Identity Management, Authentication, and Access Control)** - PR.AA-03 (Users authenticated) - PR.AA-05
Secondary NIST CSF 2.0	▪ PR.IR-01
Cisco Capabilities	▪ **Cisco Duo** – Industry-leading phishing-resistant MFA, passwordless, and adaptive authentication ▪ **Cisco Identity Intelligence** ▪ **Cisco Active Defense (AD)** ▪ **Cisco Secure Access** – ZTNA with integrated MFA enforcement ▪ **Cisco Identity Services Engine (ISE)** – Network-level MFA policy enforcement

2.4 Disable Local Administrator Accounts (Excellent)

ACSC Description: Disable or assign unique random passphrases to local administrator accounts to prevent lateral movement.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.AA (Identity Management, Authentication, and Access Control)** - PR.AA-01 - PR.AA-05
Secondary NIST CSF 2.0	▪ RS.MI-01

Mapping Layer	Detail
Cisco Capabilities	▪ **Cisco Duo** – Device trust and local account risk signal integration ▪ **Cisco Identity Intelligence** ▪ **Cisco Secure Endpoint** – Detection of local account abuse ▪ **Splunk Enterprise Security** – Supports “Disable Local Administrator Accounts” by monitoring and alerting on any local administrator account logon, enablement, or misuse to validate the control and detect policy breaches

2.5 Network Segmentation (Excellent)

ACSC Description: Deny traffic between computers unless required; constrain BYOD/IoT; restrict access to network shares.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.IR (Technology Infrastructure Resilience)** - PR.IR-01 (Networks protected from unauthorised access) ▪ **PR.AA** - PR.AA-05
Secondary NIST CSF 2.0	▪ RS.MI-01
Cisco Capabilities	▪ **Cisco Secure Firewall** – Micro-segmentation and zone-based policy enforcement ▪ **Cisco Identity Services Engine (ISE)** – Dynamic segmentation and BYOD/IoT profiling ▪ **Cisco Secure Access** ▪ **Cisco Hypershield** ▪ **Cisco Secure Workload** ▪ **Cisco Software-Defined Access (SD-Access)** – Policy-based network segmentation ▪ **Cisco Cyber Vision** – OT/IoT network segmentation visibility

2.6 Protect Authentication Credentials (Excellent)

ACSC Description: Remove CPassword values, configure WDigest, use Credential Guard, change default passwords, enforce long complex passphrases.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.AA (Identity Management, Authentication, and Access Control)** – PR.AA-01 – PR.AA-02 – PR.AA-04
Secondary NIST CSF 2.0	▪ PR.PS-01
Cisco Capabilities	▪ **Cisco Duo** – Credential protection via MFA and passwordless ▪ **Cisco Secure Endpoint** – Credential theft prevention ▪ **Splunk User Entity Behaviour Analytics** – Detection of credential harvesting activity ▪ **Splunk Enterprise Security** – Alerting on credential-based attack indicators

2.7 Non-Persistent Virtualised Sandboxed Environments (Very Good)

ACSC Description: Use virtualised sandboxed environments for risky activities such as web browsing and viewing untrusted files.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.IR (Technology Infrastructure Resilience)** – PR.IR-01 – PR.IR-03 ▪ **PR.PS** – PR.PS-01
Secondary NIST CSF 2.0	▪ PR.DS-01
Cisco Capabilities	▪ **Cisco Secure Access** – Isolation of web browsing ▪ **Cisco Secure Malware Analytics (Threat Grid)** – Sandboxed analysis environments ▪ **Cisco Secure Workload** – Workload isolation and micro-segmentation

2.8 Software-Based Firewall (Inbound Blocking) (Very Good)

ACSC Description: Block incoming malicious/unauthorised network traffic; deny by default.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.IR (Technology Infrastructure Resilience)** – PR.IR-01 ▪ **DE.CM** – DE.CM-01
Secondary NIST CSF 2.0	· PR.PS-01
Cisco Capabilities	▪ **Cisco Secure Firewall** – Stateful inspection, IPS, and default-deny policies ▪ **Cisco Secure Client** ▪ **Cisco Secure Access** – DNS-layer default-deny enforcement ▪ **Cisco Secure Workload** ▪ **Isovalent** ▪ **Cisco Multicloud Defense**

2.9 Software-Based Firewall (Outbound Blocking) (Very Good)

ACSC Description: Block outgoing traffic not generated by approved programs; deny by default.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.IR (Technology Infrastructure Resilience)** – PR.IR-01 ▪ **PR.PS (Outbound)** – PR.PS-05
Secondary NIST CSF 2.0	· DE.CM-01
Cisco Capabilities	▪ **Cisco Secure Firewall** – Outbound application-aware policy enforcement ▪ **Cisco Secure Access** – Cloud Access Security Broker (CASB) and DLP for outbound traffic; DNS and web-layer outbound control ▪ **Cisco Secure Workload**

2.10 Outbound Web and Email Data Loss Prevention (Very Good)

ACSC Description: Block unapproved cloud services; log outbound emails; block emails with sensitive data patterns.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.DS (Data Security)** – PR.DS-01 – PR.DS-02 ▪ **PR.PS** – PR.PS-05
Secondary NIST CSF 2.0	▪ DE.CM-01
Cisco Capabilities	▪ **Cisco Secure Access** – Cloud application control and Data Loss Prevention (DLP) ▪ **Cisco Secure Email** – Outbound email DLP

3. Mitigation Strategies to Detect Cybersecurity Incidents and Respond

3.1 Continuous Incident Detection and Response (Excellent)

ACSC Description: Automated real-time analysis of centralised, time-synchronised logs of events, authentication, file access, and network activity.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **DE.CM (Continuous Monitoring)** – DE.CM-01 – DE.CM-03 – DE.CM-09; ▪ **DE.AE – DE.AE-03, DE.AE-06**
Secondary NIST CSF 2.0	▪ RS.MA ▪ RS.AN
Cisco Capabilities	▪ **Splunk Core/Splunk Enterprise Security** – Centralised Security Information and Event Management (SIEM) with real-time threat detection and automated alerting ▪ **Cisco XDR** – Cross-domain detection and automated response ▪ **Splunk SOAR** – Automated orchestration of incident response ▪ **Cisco Security Analytics and Logging** – Network telemetry aggregation

3.2 Host-Based Intrusion Detection/Prevention System (Very Good)

ACSC Description: Identify anomalous behaviour during program execution including process injection and persistence.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **DE.CM (Continuous Monitoring)** – DE.CM-09 ▪ **DE.AE** – DE.AE-02 – DE.AE-07
Secondary NIST CSF 2.0	▪ RS.AN-03
Cisco Capabilities	▪ **Cisco Secure Endpoint** – Host-based Intrusion Prevention System (HIPS)/ Endpoint Detection and Response (EDR) with behavioural analysis, process injection detection, and persistence monitoring ▪ **Cisco XDR** – Host-layer telemetry correlation

3.3 Endpoint Detection and Response (EDR) (Very Good)

ACSC Description: Centralised logging of system behaviour to facilitate incident response.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **DE.CM (Continuous Monitoring)** – DE.CM-09 ▪ **RS.AN (Incident Analysis)** – RS.AN-03 – RS.AN-06 – RS.AN-07
Secondary NIST CSF 2.0	▪ RS.MA
Cisco Capabilities	▪ **Cisco Secure Endpoint** – Full EDR capability with device trajectory, file activity, and network connection logging ▪ **Cisco XDR** – Extended detection across endpoint, network, cloud, and identity ▪ **Splunk Attack Analyser** – Behavioural and forensic analysis of endpoint telemetry

3.4 Threat Hunting (Very Good)

ACSC Description: Hunt for incidents using adversary tradecraft knowledge and threat intelligence.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **DE.AE (Adverse Event Analysis)** – DE.AE-07 (Threat intelligence integration) – DE.AE-02 ▪ **ID.RA** – ID.RA-02
Secondary NIST CSF 2.0	▪ RS.AN-03
Cisco Capabilities	▪ **Cisco Talos Intelligence** – World-class threat intelligence for proactive hunting ▪ **Cisco XDR** – Threat hunting across the extended enterprise ▪ **Splunk Enterprise Security** – Threat hunting with correlation searches, data models assets and identities ▪ **Splunk User and Entity Behaviour Analytics (UEBA)** – Threat hunting using ML-driven anomaly detection, user and entity behaviour. ▪ **Splunk Attack Analyser** – Adversary tradecraft analysis

3.5 Network-Based IDS/IPS (Limited)

ACSC Description: Use signatures and heuristics to identify anomalous traffic internally and at network perimeters.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **DE.CM (Continuous Monitoring)** – DE.CM-01 ▪ **DE.AE** – DE.AE-03
Secondary NIST CSF 2.0	▪ PR.IR-01
Cisco Capabilities	▪ **Cisco Secure Firewall (with Snort IPS)** – Network Intrusion Detection System/Intrusion Prevention System (IDS/IPS) with Snort-based signature and behavioural detection ▪ **Cisco Secure Network Analytics** – Behavioural network traffic analysis ▪ **Cisco XDR** – Network detection correlation ▪ **Cisco Secure Access**

3.6 Capture Network Traffic (Limited)

ACSC Description: Capture network traffic from critical assets and perimeter to support incident detection and analysis.

Mapping Layer	Detail

Primary NIST CSF 2.0	• DE.CM (Continuous Monitoring)
	  – DE.CM-01
	• RS.AN (Incident Analysis)
	  – RS.AN-03
	  – RS.AN-07

Secondary NIST CSF 2.0	• DE.AE-03
Cisco Capabilities	• **Cisco Secure Network Analytics** – Full network telemetry capture and flow analysis • **Cisco XDR** – Network telemetry correlation • **Splunk Core** – Network traffic log aggregation and forensic analysis

4. Mitigation Strategies to Recover Data and System Availability

4.1 Regular Backups (Essential)

ACSC Description: Regular backups of data, software, and configurations; stored disconnected; retained ≥3 months; tested regularly.

Mapping Layer	Detail

Primary NIST CSF 2.0	• **RC.RP (Incident Recovery Plan Execution)**
	  – RC.RP-02
	  – RC.RP-03 (Backup integrity verified)
	• **PR.DS**
	  – PR.DS-11 (Backups created, protected, maintained, and tested)

Secondary NIST CSF 2.0	• PR.IR-03
Cisco Capabilities	• **Cisco XDR** – Ransomware Recovery with Cohesity • **Splunk Enterprise Security** – Monitoring backup job status and integrity • **Cisco Secure Endpoint** – Prevention of ransomware affecting backup systems • **Cisco Secure Firewall** – Network isolation of backup infrastructure

4.2 Business Continuity and Disaster Recovery Plans (Very Good)

ACSC Description: Tested, documented Business Continuity Plans (BCPs); printed hardcopy with offline softcopy; focus on highest-priority systems.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **RC.RP (Incident Recovery Plan Execution)** – RC.RP-01 – RC.RP-04 – RC.RP-06 ▪ **RC.CO** – RC.CO-03
Secondary NIST CSF 2.0	▪ ID.IM-04 ▪ RS.MA
Cisco Capabilities	▪ **Splunk Enterprise Security** – Operational status monitoring during recovery (governance) ▪ **Cisco XDR** – Coordinated incident response to support BCP activation ▪ **Cisco Secure Firewall** – Network recovery path enforcement

4.3 System Recovery Capabilities (Very Good)

ACSC Description: Virtualisation with snapshots, remote OS reinstallation, enterprise mobility, and vendor support contracts.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **RC.RP (Incident Recovery Plan Execution)** – RC.RP-02 – RC.RP-05 ▪ **PR.IR** – PR.IR-03 – PR.IR-04
Secondary NIST CSF 2.0	▪ RC.CO-03
Cisco Capabilities	▪ **Cisco XDR** with Cohesity – Ransomware Recovery

5. Mitigation Strategy Specific to Preventing Malicious Insiders

5.1 Personnel Management (Very Good)

ACSC Description: Ongoing vetting for privileged users; immediately disable departing user accounts; remind users of security obligations.

Mapping Layer	Detail
Primary NIST CSF 2.0	▪ **PR.AA (Identity Management, Authentication, and Access Control)** - PR.AA-01 - PR.AA-05 - PR.AA-06 ▪ **GV.RR** - GV.RR-04 (Cybersecurity included in HR practices)
Secondary NIST CSF 2.0	▪ PR.AT ▪ DE.CM-03
Cisco Capabilities	▪ **Cisco Duo** – Immediate account deactivation enforcement via MFA policy ▪ **Cisco Identity Intelligence** ▪ **Cisco Identity Services Engine (ISE)** – Rapid access revocation ▪ **Splunk User Entity Behaviour Analytics (UEBA)** – Insider threat detection and anomalous user activity monitoring ▪ **Cisco XDR** – Cross-domain insider activity correlation

[2] Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines, NIST Internal Report 8477, https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8477.pdf.

3. Cisco Security Product – Consolidated Mapping

The table below provides a high-level summary view of the full mapping of Cisco Security products that have relevance to each ACSC mitigation strategy:

ACSC Mitigation Strategy	ACSC Effectiveness	Relevant Cisco Capability
Mitigation Strategies to Prevent Malware Delivery and Execution		
Application Control	Essential	• Cisco Firewall • Cisco Secure Access • Cisco Secure Endpoint • Cisco Secure Client • Cisco Secure Email
Patch Applications	Essential	• Cisco Secure Endpoint • Cisco Secure Access • Cisco Secure Workload • Cisco Secure Network Analytics • Splunk Exposure Analytics
Office Macro Settings	Essential	• Cisco Secure Email • Cisco Secure Endpoint • Cisco Secure Access • Splunk Enterprise Security
User Application Hardening	Essential	• Cisco Duo IAM • Cisco Secure Client • Cisco Secure Endpoint • Cisco Secure Access
Sandboxing	Excellent	• Cisco Malware Analytics • Cisco Secure Email • Cisco Secure Endpoint • Cisco Secure Access
Email Content Filtering	Excellent	• Cisco Secure Email
Web Content Filtering	Excellent	• Cisco Secure Access • Cisco Secure Firewall • Cisco Meraki MX • Cisco Secure Web Appliance

ACSC Mitigation Strategy	ACSC Effectiveness	Relevant Cisco Capability
Gateway Firewall/Proxy	Excellent	• Cisco Secure Firewall • Cisco Secure Access • Cisco Meraki MX
OS Exploit Mitigation	Excellent	• Cisco Secure Endpoint • Cisco XDR • Splunk Enterprise Security
Server App Hardening	Very Good	• Cisco Secure WAF • Cisco Multicloud Defense • Cisco Secure Firewall • Cisco Secure Workload • Isovalent
OS Hardening	Very Good	• Cisco Secure Endpoint • Cisco Meraki Systems Manager • Splunk Enterprise Security
Antivirus (Heuristic)	Very Good	• Cisco Secure Endpoint • Cisco Secure Access
Control Removable Media	Very Good	• Cisco Secure Endpoint • Cisco ISE • Cisco Secure Client
Block Spoofed Emails	Very Good	• Cisco Secure Email
User Education	Good	• Cisco Duo • Cisco Secure Email with KnowB4 • Cisco Secure Access with KnowB4
AV software	Limited	–
TLS email server connections	Limited	• Cisco Secure Email

ACSC Mitigation Strategy	ACSC Effectiveness	Relevant Cisco Capability
Mitigation Strategies to Limit the Extent of Cybersecurity Incidents		
Restrict Admin Privileges	Essential	• Cisco Duo IAM • Cisco Identity Intelligence • Cisco Secure Access • Cisco ISE • Splunk UEBA
Patch Operating Systems	Essential	• Cisco Secure Workload • Cisco Hypershield • Cisco Secure Firewall • Splunk Exposure Analytics
Multi-Factor Authentication	Essential	• Cisco Duo IAM • Cisco Identity Intelligence • Cisco AD Defense • Cisco Secure Access • Cisco ISE
Disable Local Admin Accounts	Excellent	• Cisco Duo • Cisco Identity Intelligence • Cisco Secure Endpoint • Splunk Enterprise Security
Network Segmentation	Excellent	• Cisco Secure Firewall • Cisco Hypershield • Cisco ISE • Cisco Secure Workload • Cisco Secure Access • Cisco SD-Access • Cisco Application Centric Infrastructure (Cisco ACI®)
Protect Auth Credentials	Excellent	• Cisco Duo • Cisco Secure Endpoint • Splunk UEBA • Splunk Enterprise Security

ACSC Mitigation Strategy	ACSC Effectiveness	Relevant Cisco Capability
Non-Persistent Sandboxes	Very Good	• Cisco Secure Access • Cisco Malware Analytics • Cisco Secure Workload
Inbound Firewall	Very Good	• Cisco Secure Firewall • Cisco Secure Client • Cisco Secure Access • Cisco Secure Workload • Cisco Multicloud Defense • Isovalent
Outbound Firewall	Very Good	• Cisco Secure Firewall • Cisco Secure Access • Cisco Secure Workload
Outbound DLP	Very Good	• Cisco Secure Access • Cisco Secure Email
Mitigation Strategies to Detect Cybersecurity Incidents and Respond		
Continuous Detection and Response	Excellent	• Splunk Core • Splunk Enterprise Security • Splunk SOAR • Cisco XDR • Cisco Security Analytics and Logging
Host-Based IDS/IPS	Very Good	• Cisco Secure Endpoint Cisco XDR
EDR	Very Good	• Cisco Secure Endpoint • Cisco XDR • Splunk Attack Analyser
Threat Hunting	Very Good	• Cisco Talos Intelligence • Cisco XDR • Splunk Enterprise Security • Splunk UEBA • Splunk Attack Analyser

ACSC Mitigation Strategy	ACSC Effectiveness	Relevant Cisco Capability
Network IDS/IPS	Limited	• Cisco Secure Firewall • Cisco XDR • Cisco Secure Network Analytics • Cisco Secure Access
Network Traffic Capture	Limited	• Cisco Secure Network Analytics • Cisco XDR • Splunk Core
Mitigation Strategies to Recover Data and System Availability		
Regular Backups	Essential	• Cisco XDR with Cohesity • Splunk Enterprise Security • Cisco Secure Endpoint • Cisco Secure Firewall
BCP/Disaster Recovery	Very Good	• Splunk Enterprise Security • Cisco XDR • Cisco Secure Firewall
System Recovery Capabilities	Very Good	• Cisco XDR with Cohesity
Mitigation Strategy Specific to Preventing Malicious Insiders		
Personnel Management	Very Good	• Cisco Duo IAM • Cisco Identity Intelligence • Cisco AD Defense • Cisco ISE • Splunk UEBA • Cisco XDR

4. Key Observations

NIST CSF 2.0 Functions Coverage

The ACSC strategies collectively provide strong coverage across all six NIST CSF 2.0 Functions:

- **GOVERN (GV):** Addressed primarily through the non-technical strategies (Personnel Management, User Education) and the governance dimensions of privilege management.
- **IDENTIFY (ID):** Strongly addressed through patching strategies, which require robust asset and vulnerability identification.
- **PROTECT (PR):** The most heavily addressed function, with the majority of ACSC strategies mapping here — particularly PR.AA, PR.PS, and PR.DS.
- **DETECT (DE):** Directly addressed by the detection and response category strategies.
- **RESPOND (RS):** Addressed through the continuous detection/response, EDR, and threat-hunting strategies.
- **RECOVER (RC):** Addressed through the three recovery-specific strategies.

Cisco Portfolio Coverage Observations

- **Cisco Duo Identity Access Management** is the single most broadly applicable Cisco product, supporting the three Essential Eight MFA-related controls and extending across PR.AA broadly.
- **Cisco Secure Endpoint** provides foundational coverage across Prevention, Detection, and Response categories.
- **Splunk Enterprise Security and Cisco XDR** are the primary enablers of the Threat Detection and Incident Response strategy cluster.
- **Cisco Secure Firewall, Cisco Secure Workload, Cisco Secure Access, and Cisco ISE** together address the network-layer prevention strategies most comprehensively.
- **Cisco Secure Email solutions** address the email-specific ACSC strategies.

Architectural Differentiation

Three capabilities distinguish Cisco's approach from best-of-breed aggregation:

1. Network-Native Segmentation (ACSC 2.5 — Excellent)

Cisco ISE, Secure Workload, and Hypershield deliver agentless microsegmentation across IT/OT/IoT environments. Competitive approaches (CrowdStrike + Zscaler) require host agents on every endpoint — a non-starter for industrial control systems, medical devices, and legacy infrastructure common in ANZ utilities, healthcare, and transport sectors.

2. Splunk Integration for Detection/Response (ACSC 3.1–3.4)

ACSC Continuous Detection (3.1 — Excellent) requires SIEM-class log aggregation and correlation. Cisco XDR + Splunk Enterprise Security deliver this natively. Point-solution stacks (Palo Alto Cortex, Microsoft Sentinel) require custom integration overhead and lack Splunk's data platform extensibility for IT Ops and business analytics.

3. Cohesity Partnership for Backup/Recovery (ACSC 4.1 — Essential)

Essential Eight mandates tested, disconnected backups. Cisco XDR with Cohesity delivers ransomware recovery with immutable snapshots. Competitors position backup as out-of-scope (CrowdStrike) or require separate vendor relationships (Zscaler + Veeam), fragmenting the recovery workflow.

5. Close

This paper has demonstrated that the ACSC Strategies to Mitigate Cybersecurity Incidents and NIST CSF 2.0 are highly complementary frameworks. The ACSC strategies provide prescriptive, operationally focused controls that map cleanly to NIST CSF 2.0's outcome-based categories. Australian organisations can use both frameworks simultaneously without duplication of effort.

Cisco's Security portfolio provides comprehensive capability coverage across virtually all mapped control areas, with strength in Protection (PR), Detection (DE), and Response (RS) Functions. By deploying the Cisco capabilities identified in this paper, Australian organisations can simultaneously progress their ACSC Essential Eight implementation and their NIST CSF 2.0 alignment — achieving a robust, internationally recognised cybersecurity posture.

This white paper references the ASD Strategies to Mitigate Cybersecurity Incidents (February 2017), NIST CSF 2.0 (February 2024), and Cisco's Security Portfolio Mapping to NIST CSF 2.0. Organisations should consult current versions of all referenced frameworks and engage qualified cybersecurity professionals for implementation guidance.

Next steps

For Public Sector/Regulated Industry:

Use Appendix C (Product-ACSC Matrix) to assess current security stack capability coverage against Essential Eight requirements.

For Commercial/Enterprise:

Assess network segmentation capabilities — ACSC 2.5 (Network Segmentation — Excellent) is the highest-ROI control for ransomware containment.

APPENDIX A

ACSC Mitigation Strategies (Top37)

Mitigation Strategies to Prevent Malware Delivery and Execution [17]

- **Essential** Application control to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- **Essential** Patch applications (e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers). Patch/mitigate computers with “extreme risk” vulnerabilities within 48 hours. Use the latest version of applications.
- **Essential** Configure Microsoft Office macro settings to block macros from the internet, and allow only vetted macros either in “trusted locations” with limited write access or digitally signed with a trusted certificate.
- **Essential** User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads, and Java on the internet. Disable unneeded features in Microsoft Office (e.g. Object Linking and Embedding [OLE]), web browsers, and PDF viewers.
- **Excellent** Automated dynamic analysis of email and web content run in a sandbox, blocked if suspicious behaviour is identified (e.g. network traffic, new or modified files, or other system configuration changes).
- **Excellent** Email content filtering. Allow only approved attachment types (including in archives and nested archives). Analyse/sanitise hyperlinks, PDF, and Microsoft Office attachments. Quarantine Microsoft Office macros.
- **Excellent** Web content filtering. Allow only approved types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks, and free domains.
- **Excellent** Deny corporate computers direct internet connectivity. Use a gateway firewall to require use of a split DNS server, an email server, and an authenticated web proxy server for outbound web connections.
- E**xcellent** Operating system generic exploit mitigation e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR), and Enhanced Mitigation Experience Toolkit (EMET).
- **Very Good** Server application hardening especially internet-accessible web applications (sanitise input and use TLS not SSL) and databases, as well as applications that access important (sensitive/high-availability) data.
- **Very Good** Operating system hardening (including for network devices) based on a Standard Operating Environment, disabling unneeded functionality (e.g. RDP, AutoRun, LanMan, SMB/NetBIOS, LLMNR, and WPAD).
- **Very Good** Antivirus software using heuristics and reputation ratings to check a file’s prevalence and digital signature prior to execution. Use antivirus software from different vendors for gateways versus computers.
- **Very Good** Control removable storage media and connected devices. Block unapproved CD/DVD/USB storage media. Block connectivity with unapproved smartphones, tablets, and Bluetooth/Wi-Fi/3G/4G/5G devices.
- **Very Good** Block spoofed emails. Use Sender Policy Framework (SPF) or Sender ID to check incoming emails. Use “hard fail” Sender Policy Framework (SPF) TXT and DMARC DNS records to mitigate emails that spoof the organisation’s domain.
- **Good** User education. Avoid phishing emails (e.g. with links to login to fake websites), weak passphrases, passphrase reuse, as well as unapproved: removable storage media, connected devices, and cloud services.
- **Limited** Antivirus software with up-to-date signatures to identify malware, from a vendor that rapidly adds signatures for new malware. Use antivirus software from different vendors for gateways versus computers.
- **Limited** TLS encryption between email servers to help prevent legitimate emails being intercepted and subsequently leveraged for social engineering. Perform content scanning after email traffic is decrypted.

Mitigation Strategies to Limit the Extent of Cybersecurity Incidents: [10]

- **Essential** Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Do not use privileged accounts for reading email and web browsing.
- **Essential** Patch operating systems. Patch/mitigate computers (including network devices) with "extreme risk" vulnerabilities within 48 hours. Use the latest operating system version. Do not use unsupported versions.
- **Essential** Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.
- **Excellent** Disable local administrator accounts or assign passphrases that are random and unique for each computer's local administrator account to prevent propagation using shared local administrator credentials.
- **Excellent** Network segmentation. Deny traffic between computers unless required. Constrain devices with low assurance (e.g. BYOD and IoT). Restrict access to network drives and data repositories based on user duties.
- **Excellent** Protect authentication credentials. Remove CPassword values (MS14-025). Configure WDigest (KB2871997). Use Windows Defender Credential Guard. Change default passphrases. Require long complex passphrases.
- **Very Good** Non-persistent virtualised sandboxed environment, denying access to important (sensitive/high-availability) data, for risky activities (e.g. web browsing, and viewing untrusted Microsoft Office and PDF files).
- **Very Good** Software-based application firewall, blocking incoming network traffic that is malicious/unauthorised, and denying network traffic by default (e.g. unneeded/unauthorised RDP and SMB/NetBIOS traffic).
- **Very Good** Software-based application firewall, blocking outgoing network traffic that is not generated by approved/trusted programs, and denying network traffic by default.
- **Very Good** Outbound web and email data loss prevention. Block unapproved cloud computing services. Log recipient, size, and frequency of outbound emails. Block and log emails with sensitive words or data patterns.

Mitigation Strategies to Detect Cybersecurity Incidents and Respond: [6]

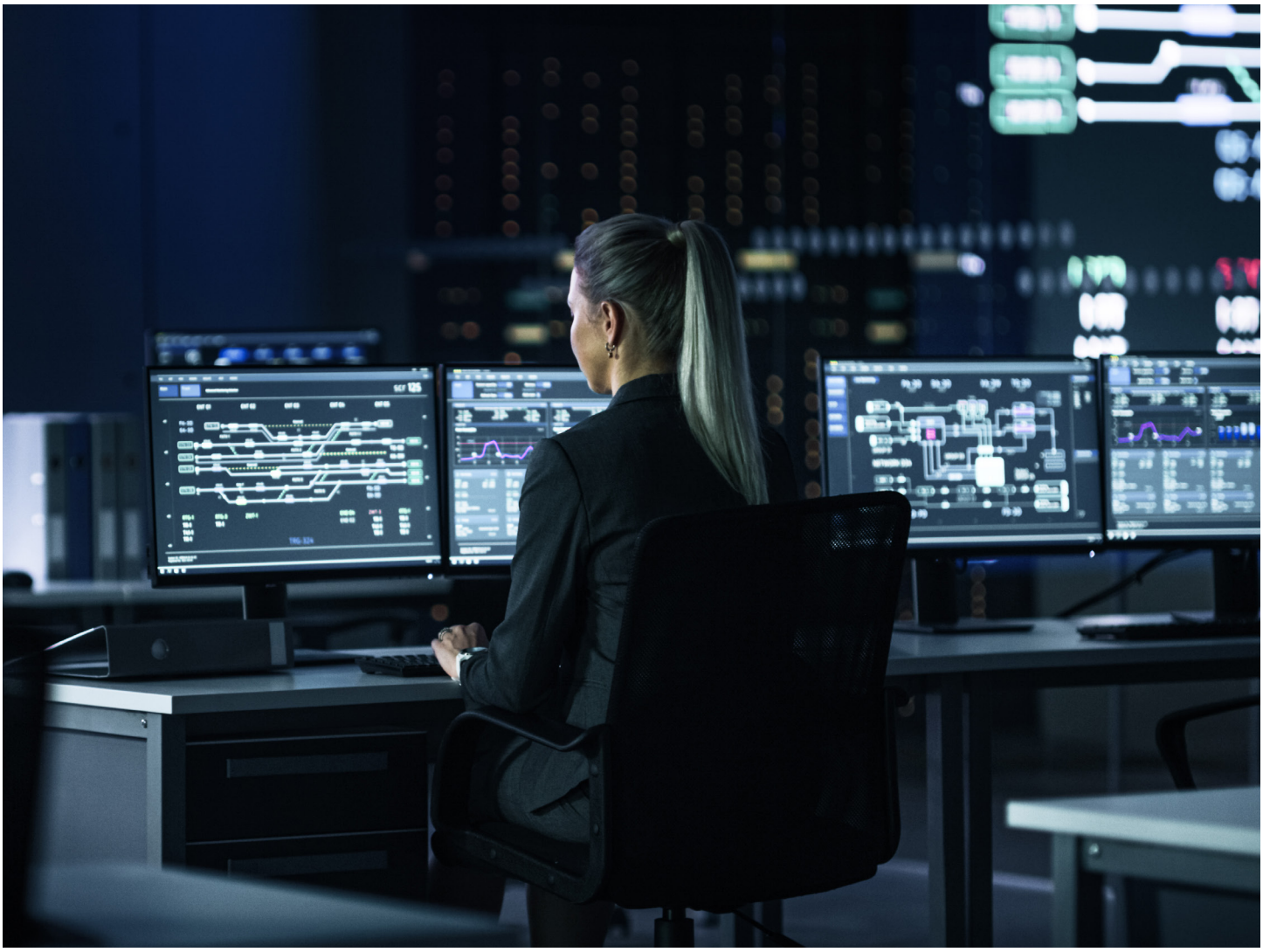
- **Excellent** Continuous incident detection and response with automated immediate analysis of centralised time-synchronised logs of allowed and denied computer events, authentication, file access and network activity.
- **Very Good** Host-based intrusion detection/prevention system to identify anomalous behaviour during program execution (e.g. process injection, keystroke logging, driver loading, and persistence).
- **Very Good** Endpoint detection and response software on all computers to centrally log system behaviour and facilitate cybersecurity incident response activities. Microsoft's free SysMon tool is an entry-level option.
- **Very Good** Hunt to discover incidents based on knowledge of adversary tradecraft. Leverage threat intelligence consisting of analysed threat data with context enabling mitigating action, not just indicators of compromise.
- **Limited** Network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- **Limited** Capture network traffic to and from corporate computers storing important data or considered as critical assets, and network traffic traversing the network perimeter, to perform incident detection and analysis.

Mitigation Strategies to Recover Data and System Availability: [3]

- **Essential** Regular backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.
- **Very Good** Business continuity and disaster recovery plans which are tested, documented and printed in hardcopy with a softcopy stored offline. Focus on the highest priority systems and data to recover.
- **Very Good** System recovery capabilities e.g. virtualisation with snapshot backups, remotely installing operating systems and applications on computers, approved enterprise mobility, and onsite vendor support contracts.

Mitigation Strategy Specific to Preventing Malicious Insiders: [1]

- **Very Good** Personnel management, e.g. ongoing vetting especially for users with privileged access, immediately disable all accounts of departing users, and remind users of their security obligations and penalties.



APPENDIX B

Cisco Product Mappings – NIST CSF 2.0

		Network Security					Device Security					User Security				Cloud Security			App Security		Analytics				Industrial Security			Other		Splunk Capabilities						
Function	**Category**	Cisco Firewalls	Cisco Defense Orchestrator	Cisco Identity Services Engine	Cisco Multicloud Defense	Cisco XDR	Cisco Secure Client	Cisco Secure Endpoint	Cisco Security Connector	Cisco Meraki Systems Manager	Cisco Duo	Cisco Secure Email Threat Defense	Cisco Secure Access (SSE)	Cisco Secure Web Appliance	Cisco Attack Surface Management	Cisco Cloud Application Security	Cisco Umbrella	Cisco Secure Workload	Cisco Secure WAF	Secure Malware Analytics	Secure Network Analytics	Security Analytics and Logging	Cisco Telemetry Broker	Cisco Industsrial Threat Defense	Cisco Cyber Vision	Secure Equipment Access	Cisco Secure Ddos Protection	Cisco Vulnerability Management	Splunk Core	Splunk Asset and Risk Intelligence	Splunk Enterprise Secuity	Splunk Attack Analyzer	Splunk User Behavior Analytics	Splunk SOAR
Govern (GV)		Non-technical controls																																	
Identify (ID)	**Asset Management (ID.AM)**	●		●	●	●	●	●	●	●	●				●	●	●	●	●		●				●	●			●	●	●		●	●
	Risk Assessment (ID.RA)	●		●		●	●	●	●		●	●	●	●	●	●	●	●		●	●	●		●	●	●		●	●	●	●	●	●	●
	Improvement (ID.IM)	Non-technical controls																																	
Protect (PR)	**Identity Management, Authentication, and Access Control (PR.AA)**	●	●	●	●		●	●	●	●	●		●	●			●	●	●	●	●	●		●	●	●	●		●	●	●	●	●	●
	Awareness and Training (PR.AT)	Non-technical controls																																	
	Data Security (PR.DS)	●	●	●	●	●	●	●	●	●	●	●	●	●			●	●	●		●			●	●	●			●	●	●		●	●
	Platform Security (PR.PS)	●	●	●	●	●	●	●		●			●	●			●	●				●	●	●		●			●	●	●		●	●
	Technology Infrastructure Resilience (PR.IR)	●	●	●	●	●	●	●	●	●	●		●	●			●	●			●	●	●	●	●	●			●	●	●	●	●	●
Detect (DE)	**Continuous Monitoring (DE.CM)**	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●
	Adverse Event Analysis (DE.AE)	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Respond (RS)	**Incident Management (RS.MA)**	Non-technical controls																																	
	Incident Analysis (RS.AN)	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●	●		●		●		●	●	●	●
	Incident Response Reporting and Communication (RS.CO)	Non-technical controls																																	
	Incident Mitigation (RS.MI)	●	●	●	●	●	●	●			●	●	●	●			●	●	●	●	●	●	●	●	●		●		●		●	●	●	●
Recover (RC)	**Incident Recovery Plan Execution (RC.RP)**		●		●	●		●		●		●					●		●			●							●	●	●	●	●	●
	Incident Recovery Communication (RC.CO)	Non-technical controls																																	

APPENDIX C

How to Use This Matrix

For RFP Responses: Copy the relevant rows for Essential Eight strategies (highlighted in blue) directly into capability coverage matrix sections. Each checkmark = product capability that addresses the control.

For Gap Analysis: Audit your current security stack against this matrix. Missing checkmarks = coverage gaps. Prioritize by ACSC Effectiveness rating (Essential > Excellent > Very Good).

For Deployment Planning: Checkmarks indicate technical capability coverage. Organisations remain responsible for configuration, testing, and validation against ACSC guidance (e.g., Duo MFA must be configured for phishing-resistant methods; ISE must be configured for role-based segmentation policies).

Cisco Product – ACSC Mitigation Strategies Matrix

ACSC Top37 Mitigation Strategies	Cisco Firewalls	Cisco Security Cloud Control	Cisco Identity Services Engine	Cisco Multicloud Defense	Cisco XDR	Cisco Secure Client	Cisco Secure Endpoint	Cisco Identity Intelligence	Cisco Duo Identity Access Management	Cisco AD Defense	Cisco Secure Email	Cisco Secure Access	Cisco Secure Web Appliance	Cisco Secure Workload	Cisco Hypershield	Isovalent	Cisco Meraki MX	Cisco Meraki Systems Manager	Cisco SD-Access and Cisco ACI	Cisco Secure WAF	Secure Malware Analytics	Secure Network Analytics	Security Analytics and Logging	Splunk Core	Splunk Exposure Analytics	Splunk Enterprise Security	Splunk Attack Analyser	Splunk User Entity Behavior Analytics	Splunk SOAR
Mitigation Strategies to Prevent Malware Delivery and Execution																													
Application Control	●	●				●	●				●	●																	
Patch Applications							●					●		●								●			●				
Office Macro Settings							●				●	●														●			
User Application Hardening						●	●		●			●																	
Sandboxing							●				●	●									●								
Email Content Filtering											●																		
Web Content Filtering	●	●					●					●	●				●	●	●										
Gateway Firewall/Proxy	●	●											●				●	●	●										
OS Exploit Mitigation					●		●																			●			
Server App Hardening	●	●		●										●		●				●									
OS Hardening							●											●	●							●			
Antivirus (Heuristic)							●					●																	
Control Removable Media			●			●	●																						
Block Spoofed Emails											●																		
User Education									●		●	●																	
AV Software																													
TLS email server connections											●																		

ACSC Top37 Mitigation Strategies	Cisco Firewalls	Cisco Security Cloud Control	Cisco Identity Services Engine	Cisco Multicloud Defense	Cisco XDR	Cisco Secure Client	Cisco Secure Endpoint	Cisco Identity Intelligence	Cisco Duo Identity Access Management	Cisco AD Defense	Cisco Secure Email	Cisco Secure Access	Cisco Secure Web Appliance	Cisco Secure Workload	Cisco Hypershield	Isovalent	Cisco Meraki MX	Cisco Meraki Systems Manager	Cisco SD-Access and Cisco ACI	Cisco Secure WAF	Secure Malware Analytics	Secure Network Analytics	Security Analytics and Logging	Splunk Core	Splunk Exposure Analytics	Splunk Enterprise Security	Splunk Attack Analyser	Splunk User Entity Behavior Analytics	Splunk SOAR
Mitigation Strategies to Limit the Extent of Cybersecurity Incidents																													
Restrict Admin Privileges			●					●	●	●		●																●	
Patch Operating Systems	●	●												●	●										●				
Multi-Factor Authentication			●					●	●	●		●																	
Disable Local Admin Accounts							●	●	●																	●			
Network Segmentation	●	●	●									●		●	●				●										
Protect Auth Credentials							●		●																	●		●	
Non-Persistent Sandboxes												●		●							●								
Inbound Firewall	●	●		●		●						●		●		●													
Outbound Firewall	●	●										●		●															
Outbound DLP											●	●																	
Mitigation Strategies to Detect Cybersecurity Incidents and Respond																													
Continuous Detection and Response					●																		●	●		●			●
Host-Based IDS.IPS					●		●																						
EDR					●		●																				●		
Threat Hunting					●																					●	●	●	
Network IDS/IPS	●	●			●							●										●							
Network Traffic Capture					●																	●		●					
Mitigation Strategies to Recover Data and System Availability																													
Regular Backups	●				●		●																			●			
DCP/Disaster Recovery	●				●																					●			
System Recovery Capabilities					●																								
Mitigation Strategy Specific to Preventing Malicious Insiders																													
Personnel Management			●		●			●	●	●																		●	

C11-5996186-00 04/26