cirrus

Cirrus Cyber Security

Services and Technology to protect and defend your organisation.

CIRRUS CYBER SECURITY

Contents

The ASD Essential 8

Cirrus Cybersecurity is based on Australian and international best practice frameworks with a proven track record of assisting organisations improve their security posture and reduce their risk.

The Cirrus team offer a comprehensive set of technology and security services to meet your needs. Our approach to security is based on best practice security frameworks such as Essential 8 and NIST. Security is not just about technology; it needs to cover a mix of people, practice, process and technology controls to effectively manage risk. We aim to understand where your business is on its security roadmap so we can assist you to progress your strategy at the pace you need.

Our highly trained staff will use the appropriate frameworks and best-of-breed security technologies to mature your posture. Prevention is the ultimate goal but this strategy needs to be coupled with a constant understanding of business risk and the ability to recover quickly should an incident occur.

DISP · ISO 27001 · Joint Cyber Security Centre · ACSC Australian Cyber Security Centre · PCI Security Standards Council · NIST National Institute of Standards and Technology · OWASP

Section 1

Advisory to help understand your current risk and develop a suitable threat defence profile

Cirrus' national team of highly experienced security professionals, coupled with a strong group of partner specialists, has the roadmap of solutions for your company's security posture. Advising current risks and the best way to defend against them, we provide strategies that helps your business reach its goals to effectively manage security.

As company networks become more interconnected, the risk to sensitive information becomes more complex. Future-Proof your business by finding out your Cyber Security Maturity.

SECURITY ASSESSMENTS

A security risk assessment identifies, assesses, and recommends security controls to minimise security threats and vulnerabilities.

COMPLIANCE

Compliance assessments analyse your businesses potential exposure to legal penalties, financial and material loss while meeting industry laws and regulations, best practices, and internal policies.

APPLICATION SECURITY

Measure an application's security maturity level and controls that prevent data or code within the app from being compromised.

DATA LOSS PREVENTION

Assessment of the controls being used to detect and prevent data breaches, malicious actors, or unwanted destruction of sensitive data to protect and secure, and comply with regulations.

POLICIES

Advice on the designing of a Security Policy which addresses requirements of your business systems, understanding the constraints on functions and process flows, access by external systems, programs and access to data by staff or 3rd parties that need to be incorporated to ensure continued business operations and success.

PENETRATION TESTING

Cirrus penetration testing is a simulated cyberattack against your business computer systems or network, to check for exploitable vulnerabilities.

VULNERABILITY

Cirrus evaluates if your system is susceptible to any known vulnerabilities and, if so, assign severity levels to those vulnerabilities, and recommend remediation or action.

Section

2

Integration of detection, prevention, and restoration solutions through experienced Technology Professionals

Good technology integration isn't about using the latest hype trend, it's about using highly certified and capable Cirrus team members with a strong project management ethos. Get an understanding how security integration can contribute to your security visibility, compliance, and protection.

Inadequate professional development and training can be one of the major obstacles for productively and growth within a business.

TECHNICAL SECURITY DEPLOYMENT

Define, design and implement a range of best-practice security technologies to assist in identifying, protecting, detecting, responding or recovering from security threats and events.

SECURITY RESIDENCY SERVICES

Organisations often require access to scarce or specialised security skills to optimise configurations, undertake security processes and supplement a customer internal capability to maintain and improve the security posture.

Section

3

Management of your security environment through both reactive and proactive measures

Take away the stress and reduce your risk by leveraging Cirrus to monitor and manage your security technologies. This can be as simple as managing a firewall to providing Network, SOC, SIEM or vulnerability services. Allow your team to focus on more strategic, innovative, and revenue-driving tasks while taking comfort that Cirrus has your back. We can deliver efficient, cost-effective and flexible support services which align with industry standards and practices.

Companies turning to a third-party managed security service provider have grown dramatically in a short space of time as the realisation of ever-changing technologies and staff is not always a cost-effective solution.

SECURITY OPERATIONS CENTRE (SOC)

Cirrus' SOC team are responsible for detecting, preventing, investigating, and responding to your cyber threats 24/7.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Software solutions that aggregate and analyse activity from many different resources across your entire IT infrastructure, collecting security data from network devices, servers, domain controllers, and more.

INCIDENT RESPONSE

Quickly identify an attack, minimise its effects, contain any damage caused and remediate to reduce future incidents.

VULNERABILITY AS A SERVICE (VAAS)

Identify, prioritise, and respond to vulnerability exposure across your network.

SERVER, ENDPOINT AND APPLICATION PATCHING

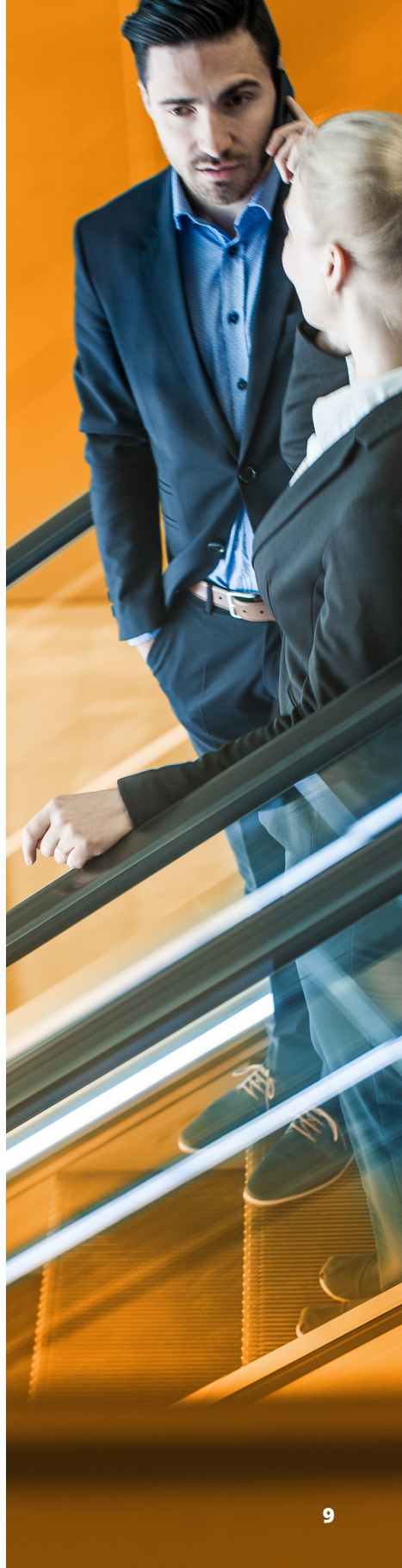
Ensure your endpoints are always running the latest approved versions by running security patches and third-party applications. Cirrus protects your devices from vulnerabilities and ensure compatibility.

ACCESS CONTROL

A fundamental component of data security, dictating who's allowed to access and use company information and resources.

BACKUP CONTROL AND PROTECTION

With hackers now focused on attacking your backup environments, Cirrus will manage, control and identity user access, protecting critical backups.



Section

4

Security Solutions for your Network

Have the visibility and the control needed to achieve good IT hygiene, starting by freeing up cluttered environments and having an effective security strategy through Cirrus.

With network architecture being so complex these days with the emergence of hybrid and software define connectivity, there are a broad range of unidentified threats that can exist.

NETWORK VISIBILITY AND SECURITY

Have visibility of your data within your network and mitigate any cyber security incidents.

MICRO-SEGMENTATION

Create zones in data centres and cloud environments to isolate workloads from one another and secure them individually on a Zero Trust approach.

WIRELESS SECURITY

Prevent unauthorised access or damage to computers or data using wireless networks such as Wi-Fi.

FIREWALL AND GATEWAY

Secure your network from internet hacking or spam traffic bots.

INTRUSION DETECTION AND PREVENTION

Monitor events in your network and analyse for signs of possible incidents, violations, or imminent threats to your security.

IDENTITY SERVICES

Ensure users are who they claim to be and give access to software applications, files and other resources at the given times.

CROSS-DOMAIN SOLUTIONS (CDS)

Allow a trusted network to exchange information with other domains, either one-way or bidirectionally, without introducing the potential for security threats that would come with network connectivity.

Section

5

Security Solutions for Hybrid Environments

Keep your sensitive or regulated data on-premise, in your IT environment where security standards are critical, while leveraging cloud resources to distribute apps, workloads and data that are not subject to cybersecurity regulations.

The new norm for employees to access corporate information and applications, anywhere, at any time, requires serious consideration as businesses collaboration, innovate, differentiate, and retain talent.

ENDPOINT PROTECTION

Security solutions to address securing and protecting Endpoints against exploits, attacks and data leakage resulting from human error.

APPLICATION SECURITY AND WHITELISTING

Whitelist approved software or files that are active on the business computer system and stop potentially harmful applications.

DATA LOSS PREVENTION

Detect and prevent data breaches, malicious actors, or unwanted destruction of sensitive data to protect and secure and comply with regulations.

MULTI-FACTOR AUTHENTICATION

Implement a security measure that requires two or more proofs of identity to grant staff access.

VULNERABILITY MANAGEMENT

Identify, prioritise and respond to vulnerability exposure across your network.

INTERNET OF THINGS (IOT) AND OPERATIONAL TECHNOLOGY (OT) SECURITY

Monitor and control the performance of your physical devices.

Connecting without Boundaries

cirrusnetworks.com.au