Kyle Griffin, Tereza Prochazkova, Torin Flanagan

Keg0215@student.usc.edu.au, t\_p111@student.usc.edu.au , tdf008@student.usc.edu.au

Student IDs: 1137837, 1173943, 1169130  
Campus: Sippy Downs  
Tutor’s name: Shena Machin  
Due date: 17/09/2025  
Submission date: 17/09/2025  
Word Count: 2,769

Task 2 – Cyber Security Defence Plan

SEC 200: Cyber Security

# Executive Summary

In response to escalating cyber threats against critical infrastructure, particularly from nation-state adversaries, OURGAS has developed a comprehensive Cyber Security Defence plan. Authorised by senior management and informed by guidance from the Australian Signals Directorate (ASD), this plan has been tailored to realistically meet the requirements that a medium-sized Australian petroleum distributor must comply with.

The defence strategy aligns with the globally recognised framework, NIST Cyber Security Framework, and the Australian Energy Sector Cyber Security Framework (AESCSF), enabling a structured, industry-aligned, and risk-based approach to cyber resilience.

The plan is built upon the assumption of full organisational commitment, stable operations, and compliance with all applicable Australian cybersecurity regulations. While it is unreasonable to assume complete protection, this plan maximises OURGAS’s ability to detect, contain, and recover from incidents, contributing to the preservation of operations, shareholder confidence, and regulatory compliance.

Through actionable, cost-effective, and scalable cyber defence measures, OURGAS is positioned to uphold its critical role in Australia's energy sector while mitigating evolving cyber risks.

The content of this report focuses on the following areas:

* Identification of critical assets across both IT and OT environments, including SCADA systems, legacy infrastructure, and third-party dependencies.
* Protection and detection through layered network security, endpoint protection (EDR/AV), secure data handling with encryption, RBAC/ABAC access controls, and proactive monitoring via SIEM with threat intelligence integration.
* Human factor mitigation through targeted security awareness programs, phishing training, and cultural transformation policies that embed cyber hygiene into daily operations.
* Incident response structured under a detailed incident response plan (IRP) outlining defined roles, detection procedures, communication protocols, and containment strategies to minimise operational impact.
* Recovery and continuity plans that prioritise verified backups, hardened system restoration, and post-incident reviews to improve resilience and operational preparedness.
* Strategic planning of resource allocation, employment of skilled personnel, layered hardware/software controls, budget forecasting, and a realistic timeline of asset implementation

Table of Contents

[Executive Summary i](#_Toc209013997)

[1 Introduction 1](#_Toc209013998)

[1.1 Authorisation and Purpose 1](#_Toc209013999)

[1.2 Scope 1](#_Toc209014000)

[1.3 Limitations 1](#_Toc209014001)

[1.4 Assumptions 1](#_Toc209014002)

[2 Defence Plan & Analysis 2](#_Toc209014003)

[2.1 Identify 2](#_Toc209014004)

[2.1.1 Assets 2](#_Toc209014005)

[2.1.2 Threats & Vulnerabilities 2](#_Toc209014006)

[2.1.3 Business Impact 2](#_Toc209014007)

[2.2 Protect & Detect 3](#_Toc209014008)

[2.2.1 Network Security Measures 3](#_Toc209014009)

[2.2.2 Data Security Protocols 3](#_Toc209014010)

[2.2.3 Endpoint Security 4](#_Toc209014011)

[2.2.4 Human Factors 5](#_Toc209014012)

[2.3 Respond 6](#_Toc209014013)

[2.3.1 Response Planning 6](#_Toc209014014)

[2.3.2 Communications 7](#_Toc209014015)

[2.3.3 Analysis 8](#_Toc209014016)

[2.3.4 Mitigation & Containment 8](#_Toc209014017)

[2.4 Recovery 10](#_Toc209014018)

[2.5 Planning & Resource Allocation 11](#_Toc209014019)

[2.5.1 Required Personnel, Hardware & Software 11](#_Toc209014020)

[2.5.2 Budget Considerations 12](#_Toc209014021)

[2.5.3 Implementation Timeline 13](#_Toc209014022)

[2.6 Justification 14](#_Toc209014023)

[3 Conclusion 15](#_Toc209014024)

[4 Recommendations 15](#_Toc209014025)

[5 References 16](#_Toc209014026)

[6 Appendices 19](#_Toc209014027)

[7 AI Acknowledgement 23](#_Toc209014028)

# Introduction

## Authorisation and Purpose

Following warnings from the Australian Signals Directorate about nation-state threats to critical infrastructure, particularly OURGAS, senior management has authorised appropriate action. A comprehensive cybersecurity defence plan will be developed to address human and technical vulnerabilities, strengthen OURGAS’ security posture, mitigate risks, and ensure uninterrupted petroleum processing, storage, and delivery operations.

## Scope

Evaluating potential attack vectors is essential for developing a cyber defence plan tailored to OURGAS. The plan will focus on network security, data protection, endpoint hardening, and human factors, outlining required resources, processes, and budget within the constraints of a medium-sized petrochemical organisation. This enables the implementation of actionable, cost-effective, and sustainable security measures within current operations.

## Limitations

All recommendations are based on simulated scenarios, industry frameworks, and academic research, not live penetration tests on OURGAS infrastructure. Resources reflect a typical medium-sized petrochemical organisation, so budget or staffing changes may vary. While strategies are comprehensive, absolute immunity from nation-state threats is not guaranteed, being focused on risk mitigation and resilience.

## Assumptions

* Resource Availability: OURGAS has sufficient financial and human resources, including trained IT personnel, security software, network infrastructure, and hardware upgrades.
* Regulatory Alignment: Compliance with Australian cybersecurity regulations and recognised frameworks (e.g., NIST, AESCSF) is mandatory.
* Organisational Commitment: Senior management and employees are committed to implementing cyber defence strategies, supporting human-factor measures, security awareness, policy compliance, and reporting.
* Stable Operations: Day-to-day operations remain stable, allowing security implementations with minimal disruption to petroleum processing, storage, and delivery.
* Operational Technology: OT/SCADA devices are deployed at operational sites and segregated from IT systems.

# Defence Plan & Analysis

To meet national standards, OURGAS’ cyber defence plan aligns with NIST and AESCSF frameworks. The NIST framework helps manage cybersecurity risks across six functions: govern (strategy, policies, roles), identify (asset and risk evaluation), protect (safeguards), detect (threat analysis), respond (incident management), and recover (system restoration), providing a whole lifecycle approach to strengthen security (NIST, 2024). AESCSF, tailored for the Australian energy sector, enables self-assessment of cybersecurity practices, maturity evaluation, and identification of improvement areas, supporting OURGAS towards enhancing organisational capabilities (AEMO, 2025).

## Identify

### Assets

OT includes refinery control systems, SCADA, industrial sensors, and PLCs, while IT covers corporate networks, databases, and email servers. Data assets comprise customer and employee records (including PII), operational, and financial data. Infrastructure assets include the Perth headquarters, multiple refineries (Perth and Queensland), and storage/distribution facilities nationwide.

### Threats & Vulnerabilities

OURGAS may face APTs from nation-state adversaries. Likely attack vectors include phishing, social engineering, malware/ransomware on OT/IT, DDoS on critical services, insider threats, and supply chain attacks. Exploitable vulnerabilities include legacy OT systems, remote access points (VPNs, contractor logins), human factors (poor cyber hygiene, weak passwords, policy neglect, phishing susceptibility), weak network segmentation, and third-party dependencies (ISPs, cloud services, vendors).

### Business Impact

A successful compromise could cause operational downtime, disrupt petroleum processing and delivery, and result in revenue loss, reputational damage, stakeholder distrust, and potential regulatory fines.

## Protect & Detect

### Network Security Measures

As the primary entry and lateral movement opportunity, OURGAS networks will be secured with up-to-date measures to counter diverse attack vectors (Fortinet, 2025a).

**Firewalls:** OURGAS will deploy NGFWs from multiple vendors to reduce vendor-specific risks and ensure failover redundancy. These firewalls will perform deep packet inspection, intrusion prevention, and secure application control, while stateful and circuit-level firewalls track sessions and filter packets to prevent hijacking. Web application firewalls will protect web servers and SCADA systems from injections and XSS (Fortinet, 2023).

**Network Edge Security Controls:** Public-facing services will be isolated in a DMZ to reduce compromise risks. A proxy server will filter requests and enforce policies, while NAT masks internal IPs. A bastion host provides a hardened gateway for secure remote admin access (Dolnicek, 2024). DDoS mitigation will be outsourced to ISPs/cloud, with dual ISPs at critical sites for redundancy.

**Network Segmentation and Access Controls:** Internal networks will be segmented by department using subnets and VLANs, with guest Wi-Fi and IoT devices assigned to isolated VLANs. All wireless connections will use WPA3 for secure authentication. Adopting a zero-trust approach ensures all packets are verified, while the PoLP limits user access. Remote access will be provided via VPNs with IPSec and MFA, restricting connections to only essential systems (ASD, 2021).

**Protocol and Traffic Security:** OURGAS will use only secure protocols, including TLS, SFTP, HTTPS, and IPsec, while disabling insecure ones like Telnet. IDS/IPS solutions will monitor and block suspicious traffic, and a SIEM with threat intelligence will handle logging and alerts. Email and web gateways will filter phishing, malware, and malicious sites (Cloudflare, 2025).

### Data Security Protocols

Data security governs how information is stored and accessed. It covers data storage (physical and digital) and access control. Proper implementation reduces risks of loss, unauthorised access, and insider threats. OURGAS will enforce storage and access protocols along with network segmentation to ensure secure and efficient operations.

**Data storage:** OURGAS stores operational, financial, and personnel data, requiring secure storage and controlled access. ASD mandates that symmetric AES encryption is a necessity against current attacks (ASD, 2025), where only valid OURGAS network users can access databases, while external users must utilise RSA encryption keys. Additionally, implementing the 3-2-1 backup strategy (three copies in two locations, with one offsite) ensures redundancy against disasters and possible attacks.

**Access control:** Employees will only access data relevant to their roles, enforced through RBAC for role-based permissions and ABAC for contextual factors like user type, location, and access time (SailPoint, 2023). PoLP ensures minimum necessary privileges, reducing the risk of unauthorised access or privilege escalation. Administrative rights will be limited, monitored, and managed via separate admin accounts with regular access reviews to protect critical systems.

### Endpoint Security

Endpoint security protects devices (laptops, servers, mobile devices, etc) connected to the OURGAS network (wired/wireless) from adversary exploitation, as such endpoints serve as entry points to internal systems (Kamruzzaman et al., 2022).

**EDR and SIEM:** EDR tools will continuously monitor all OURGAS endpoints for events, processes, and network traffic. Once integrated with SIEM systems, they provide a centralised view of security events, enabling analysis and correlation with external logs (Microsoft, 2025).

**AV, Anti-Malware, and AI Behavioural Analytics:** Signature-based AV will protect all OURGAS endpoints from known threats, while anti-malware will enable heuristic detection of unknown threats. AI and behavioural analytics using ML will further analyse endpoint data to identify abnormal patterns and user behaviours (Amrez, 2024).

**Patch Management, MFA, and Encryption:** Patch management will ensure all OURGAS endpoints are updated to reduce vulnerabilities, scaling down the attack surface. MFA will be enforced for user sign-ins, with PoLP applied to relevant user roles. AES and RSA encryption algorithms will secure endpoint data transmission for at rest and in transit (Canvas, 2024).

**Cyber Security Training and Zero-Trust Architecture:** OURGAS endpoint security training will be tailored to device interactions, with zero-trust principles limiting user access to only necessary resources, reducing privilege abuse, unauthorised access, and insider threats (Palo Alto, 2015).

### Human Factors

The human factor is often the weakest link in the network. In 2024, 74% of CISOs cited human error as their greatest security threat (Proofpoint, 2024), and 29% of data breaches arose directly from human error (OAIC, 2025). Strengthening human factors will require robust policies and targeted cybersecurity training, alongside persistent future adaptations.

**Policies and Culture:** By implementing carefully selected and enforced policies, OURGAS will promote strong cyber hygiene. Ineffective or disapproved policies reduce compliance, while a lack of repercussions normalises poor behaviour, and procedures hindering productivity are often ignored (Widdowson, 2025a). Education and training will ensure users understand policy purposes. Core policies will address access control (need-to-know), secure passwords (complexity, rotation, non-sharing), and BYOD governance (personal device risks).

**Education:** Comprehensive cyber education for all OURGAS employees will strengthen the network and encourage policy compliance, reinforcing a strong security culture. Training must emphasise the individual being a key defence layer, as gaps occur when understanding or content quality is lacking (Widdowson, 2025b). Programs will cover phishing, social engineering, AI threats (e.g. prompt injection), data handling, incident response, MFA, and privacy management (e.g. social media). Embedding these practices into daily operations reduces human error, fosters a security-conscious workforce, and ensures long-term resilience through periodic refreshers and leadership support.

## Respond

The response phases define OURGAS’ structured approach to cyber incidents, detailing the IRP with team roles, detection, analysis, communication, containment, and recovery procedures. The goal is to manage incidents effectively, comply legally, minimise disruption, and continuously improve the IRP.

### Response Planning

The IRP for OURGAS provides a structured response to cyber-attacks, aligning with the NIST “Respond” phase to outline actions upon detecting an incident (NIST, 2024). It guides procedures to minimise damage and remediate compromised system vulnerabilities (ACSC, 2023).

|  |  |  |
| --- | --- | --- |
| **Incident Response Team (IRT)** | | |
| **Name** | **Role Description** | **Responsibilities** |
| Incident response manager | Leads response team. | Coordinate team, make decisions, report to management. |
| Cyber security analysts | Monitors threats. | Detect, analyse, contain, mitigate incidents. |
| System/network administrators | Manages systems/networks. | Support affected systems, implement recovery, restore services. |
| Application/database administrators | Manages applications/databases. | Identify vulnerabilities, restore systems. |
| Legal/compliance officer | Ensure legal/regulatory compliance. | Advise on obligations, reporting, assess legal risks. |
| Communications/PR Officer | Manages messaging. | Inform stakeholders, coordinate communications. |
| Human resources representative | Employee oversight. | Investigate insider threats, enforce policies. |
| Third-party vendors/contractors | External support. | Assist with cloud/vendor systems and recovery. |

*Table 1: IRT*

**Incident Detection and Analysis Procedures:**

1. Tools for monitoring cover and include EDR, SIEMs, IDPSs, NGFWs, email and web gateways, DDoS monitoring (ISP/cloud-based), OT/IT, user behaviour analytics, patch management, and human factors.
2. Areas to cover include IT infrastructure, OT and industrial systems, network and perimeter securities, human factors, and third-party/supply chain involvement.
3. OURGAS logs will need to be collected from the network, IT/OT, endpoints, cloud/third parties, and human activities to identify suspicious activity.
4. Configurations for alerts will need to be associated with OURGAS activities such as unusual user behaviour, abnormal network traffic, unauthorised access to IT/OT systems, etc.
5. Threat feeds and known vulnerability databases are to be used accordingly with OURGAS defence intelligence.
6. OURGAS security analysts are to perform root cause analysis, validate alerts, and determine the scope/impact of incidents.
7. All incidents are to be logged with relevant details and later audited.

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident Description** | **Likelihood** | **Potential Impact** | **Priority** |
| Malware infection on endpoint | high | medium | high |
| Unauthorised access attempt | medium | high | high |
| Ransomware attack | medium | critical | critical |
| OT/IT compromise | low/medium | critical | critical |
| DoS/DDoS attack | low | high | medium |
| Data breach/exposure | low | critical | critical |
| Phishing employees | high | low | medium |
| System misconfiguration downtime | medium | medium | medium |
| Insider threat/malicious activity | low/medium | high | high |
| Supply chain attack | low | high | medium |

*Table 2: Incident detection and analysis procedures*

### Communications

The OURGAS Incident Response Plan (IRP) outlines clear communication protocols to ensure coordinated and timely responses during incidents. Internally, all incidents must be reported through a defined chain of command; cybersecurity analysts notify the Incident Response Manager, who escalates to relevant leads. Timeframes for reporting are based on incident severity to enable swift action. Externally, the Communications/PR and Legal Officers handle public and third-party notifications. This includes informing clients, regulators, and partners within required legal timeframes, such as the 72-hour window for notifiable data breaches. All messaging must be approved to ensure compliance and consistency. The communications component of the IRP ensures that OURGAS maintains transparency, meets legal obligations, and preserves trust with stakeholders throughout the incident lifecycle.

### Analysis

The Analysis phase plays a critical role in understanding the scope, origin, and impact of a security incident. Upon detection, the incident response team will initiate a comprehensive investigation using data collected from across the OURGAS environment. Log sources include SIEM alerts, firewalls and IDPS data, EDR tools, and user behaviour analytics. This ensures visibility into suspicious activity such as abnormal network traffic, unauthorised access attempts, system misconfigurations and phishing threats.

Each incident is classified using pre-established criteria outlined in the IRP, dictating the required actions. Incidents are documented as they are occurring, with analysts validating alerts, identifying affected systems, and assessing indicators of compromise. All findings are recorded for compliance and audit purposes. The outcome of the analysis directly informs subsequent response phases, ensuring a cohesive and intelligence-led incident management process.

|  |  |
| --- | --- |
| **NIST Stage** | **Purpose** |
| Investigate | Investigating the scope and impact of incidents using available logs. |
| Identify | Identifying affected systems, users, and data. |
| Assess | Assessing indicators of compromise (IoCs) and attack vectors |
| Classify | Classifying the incident based on severity and system criticality. |
| Document | Documenting all findings in real time for compliance and post-incident review. |

*Table 3: Incident analysis stages*

### Mitigation & Containment

To contain the area of compromise and mitigate its impact, compromised systems will be isolated and disconnected from the network. Accounts will have MFA reset and compromised credentials disabled. Malicious traffic will be blocked with firewall rules against IPs, domains, ports, and or geo-locations. Exfiltration channels will be disabled, with encryption keys rotated for sensitive data at rest. Critical systems will fail over to backups or redundant infrastructure to maintain availability (ASD, 2017; NIST, 2024).

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident Description** | **Containment Strategy** | **Assigned To** | **Priority Level** |
| Malware infection on endpoint. | Isolate infected device from network.  Block malicious processes.  Run AV/anti-malware and EDR scans. | Cyber security analysts. | High. |
| Unauthorised access attempt. | Disable compromised accounts.  Reset credentials.  Increase logging and monitoring. | Incident response manager.  Cyber security analysts. | High. |
| Ransomware attack. | Isolate affected systems.  Restore from backups.  Remove malware.  Notify stakeholders. | Incident response manager.  Cyber security analysts. | Critical. |
| OT/IT compromise. | Disconnect affected OT/IT systems from network.  Apply emergency patches.  Monitor for abnormal commands. | Cyber security analysts. | Critical. |
| Dos/DDoS attack. | Filter/block malicious traffic.  Rate-limit connections.  Engage ISP for traffic scrubbing. | System/network administrator. | Medium. |
| Data breach/exposure. | Restrict access to compromised systems.  Preserve evidence.  Notify compliance/legal.  Prevent further exfiltration. | Legal/compliance officer.  Cyber security analysts. | Critical. |
| Phishing employees. | Quarantine malicious emails.  Block sender domain.  Notify users.  Force password resets if needed. | Communications/PR officer.  Cyber security analysts. | Medium. |
| System misconfiguration downtime. | Roll back to previous configurations.  Apply fixes.  Validate system functionality. | System/network administrator. | Medium. |
| Insider threat/malicious activity. | Suspend user account/s.  Review logs.  Investigate unusual behaviour.  Limit access. | Human resources representative.  Cyber security analysts. | High. |
| Supply chain attack. | Isolate affected vendor systems.  Audit incoming updates.  Increase monitoring of vender interactions. | Cyber security analysts. | Medium. |

*Table 4: Mitigation and containment strategies*

## Recovery

OURGAS must begin recovery once the incident is stabilised, minimising operational disruption. Verified backups are used if required, with patches applied and systems hardened before restoration. Any malware or tampering in backups must be removed. Systems are restored in priority order with OT first, followed by business IT and support functions. Enhanced monitoring and logging are maintained to prevent recurrence. All recovery steps are documented, capturing actions, timelines, and decisions for post-incident review. Finally, improvements are implemented through updated policies, patch management, training, and revised response playbooks based on lessons learned.

## Planning & Resource Allocation

### Required Personnel, Hardware & Software

**Personnel**

OURGAS requires one incident response manager to lead and coordinate the response, making key decisions. Four cybersecurity analysts will investigate alerts, analyse logs, detect intrusions, and contain threats, with responsibilities divided across network monitoring, endpoint protection, and overall security analysis. Two system/network administrators will restore and secure OT/IT infrastructure, apply patches, and manage configurations, supported by two application/database administrators to maintain data integrity, functionality, and recovery. One legal/compliance officer will ensure regulatory adherence and evidence handling, while one communications/PR officer manages internal and external communications. A single HR representative will address employee-related matters. Third-party vendors or contractors will be engaged only when specialised expertise, forensic support, or vendor-specific fixes are required.

**Hardware**

OURGAS must adopt a layered firewall strategy to protect OT and IT environments, using NGFWs such as FortiGate (Fortinet, 2023) or Cisco Firepower (Cisco, 2025) for threat detection, intrusion prevention, and application control. In addition, ruggedised OT firewalls like Fortinet Rugged (Fortinet, 2023) or Cisco ISA (Cisco, 2025) will secure SCADA and industrial networks. Internal firewalls will segment IT and OT zones, while cloud-native firewalls secure hybrid services. Network security is further enhanced through proxy servers, bastion hosts, and a DMZ. Forward proxies are used to filter outbound traffic while reverse proxies help protect server identities (Radware, 2024; Cloudflare, 2025b). Bastion hosts will then provide controlled access with MFA and hardened configurations (Microsoft, 2023). DMZs then isolate all public-facing servers from internal networks (Barney, 2021).

A 3-2-1 backup strategy will safeguard critical data by maintaining three copies: a primary copy, a local backup on a NAS or SAN for rapid recovery, and a secondary copy on different media, with a third copy securely stored offsite or in the cloud using encryption and access controls (Pusin, 2022). Finally, endpoint protection hardware, including encrypted desktops and laptops, ruggedised OT devices, and mobile device management appliances, will secure all devices accessing OURGAS systems, enforce policies, monitor compliance, and prevent unauthorised access.

**Software**

OURGAS must implement a comprehensive cybersecurity stack to protect all OT/IT systems. This includes SIEM integrated with threat intelligence for real-time monitoring, EDR capabilities, unified AV and anti-malware suites, and patch management platforms to address vulnerabilities. Remote access is secured with MFA and VPNs utilising IPSec protocols, while TLS, HTTPS, and SFTP also help protect data in transit. Access control is to be enforced through RBAC and/or ABAC systems, supported by ongoing security awareness training to maintain staff compliance and vigilance.

### Budget Considerations

Budget allocation for cybersecurity at OURGAS must reflect the organisation's reliance on critical infrastructure, particularly OT/SCADA systems, and the high value of its operational and personal data. Budget estimates should consider initial setup costs (CapEx), annual recurring costs (OpEx), and contingency reserves for emergency incident response or breach remediation (Sap Concur, 2025).

|  |  |  |
| --- | --- | --- |
| **Category** | **Item** | **Cost frequency and type** |
| Personnel | Cybersecurity analysts, system/network admins, IRP team roles. | Fixed OpEx |
|  | Third-party vendors/consultants | Variable OpEx |
| Training &  Awareness | Cybersecurity awareness & training platform subscription | Fixed OpEx |
|  | Internal awareness campaigns and simulations | Periodic OpEx |
| Hardware | NGFW from multiple vendors for redundancy | One-time CapEx |
|  | Proxy servers, DMZ infrastructure, bastion hosts | One-time CapEx |
|  | Backup storage systems | On-site: One-time OpEx  Offsite: Fixed OpEx |
|  | Secure endpoint devices | One-time CapEx |
| Software & | SIEM platform with threat intelligence | Fixed OpEx |
| Licenses | EDR, antivirus, anti-malware suites | Fixed OpEx |
|  | VPNs, MFA systems | Fixed OpEx |
|  | Access control solutions (RBAC/ABAC) | Fixed OpEx |
|  | Encryption tools | One-time CapEx |
|  | Patch management & AI behavioural analytics | Fixed OpEx |
| Compliance & Legal | Legal consulting for breach notifications | Variable OpEx |
|  | Incident documentation & audit trail tools | Fixed OpEx |
|  | Certification and framework alignment (e.g. NIST, AESCF) | Periodic CapEx |
| Contingency Reserve | Emergency incident response funds set aside for critical response and recovery | Variable CapEx |

*Table 5: Associated cost frequencies and types*

### Implementation Timeline

To implement the security measures mentioned earlier, OURGAS will adopt a phased approach. This order ensures that key protections are implemented early, while more advanced and resource-intensive measures are gradually introduced, with ongoing efforts sustained over the long term.

|  |  |  |
| --- | --- | --- |
| **Phase** | **Activities** | **Responsibility** |
| Immediate  (0-3 months) | Deploy MFA, patch management, antivirus and anti-malware solutions, implement VPN with IPsec + MFA, engage in awareness training, enable email/web filtering, outsource DDoS protection to ISP/cloud, disable legacy protocols, configure SIEM systems, and conduct phishing awareness campaigns. | IT Security, Network Security, HR |
| Short-term  (3-6 months) | Install NGFWs, establish DMZ, NAT, proxy, bastion hosts, segment with VLANs, apply RBAC and PoLP, rollout 3-2-1 backup strategy, run initial penetration tests and IRP tabletop exercise. | Network Security, Data Management |
| Medium-term  (6-12 months) | Integrate EDR with SIEM, apply AI analytics for anomalies, perform advanced employee training, deploy dual ISPs, and strengthen OT isolation. | Security Operations, OT Teams |
| Ongoing  (12+ months) | Regular penetration testing, IRP and red team exercises, rotate encryption keys, review privileges, continue advanced training, enforce policy compliance, and expand supply chain security programs. | All departments, CISO |

*Table 6: Activity implementation timeline*

## Justification

The threats OURGAS faces come from nation-state adversaries, so security measures must be strong and practical while still being feasible to implement, balancing the resource constraints of a medium-sized petroleum organisation. The defensive strategies were selected to address the threats and vulnerabilities outlined in section 2.1 and to provide layered, cost-effective protection.

Network security measures, such as NGFWs, segmentation, DMZs, and VPNs, were selected because public-facing OURGAS networks serve as primary entry points and key vectors for lateral movement. These solutions were prioritised over perimeter-only defences, as they provide stronger and more comprehensive control and protection over OT/IT networks.

Data security protocols, including AES encryption, RBAC/ABAC, and the 3-2-1 backup strategy, were selected to prevent data loss, mitigate ransomware impact, and combat insider threats, while being in line with ASD guidelines and standard industry practices.

Endpoint security solutions, such as EDR, SIEM, patch management, and MFA, help combat phishing, malware, and zero-day exploits, reducing the risk of compromise and enabling rapid detection.

Lastly, human factors were addressed through persistent awareness training and cultural reinforcement, as human error is consistently the primary cause of breaches in Australia.

Together, these measures align with the NIST Framework and AESCSF, enhancing OURGAS’ resilience and reducing the risk of compromise, thereby ensuring ongoing and secure operations.

# Conclusion

The OURGAS cyber defence plan presents a structured, realistic approach to mitigating risks posed by nation-state actors targeting critical infrastructure. By aligning with the NIST and AESCSF frameworks, this plan ensures a balanced focus on prevention, detection, response, and recovery. Through layered technical controls, strong human-factor policies, and continuous training, OURGAS can improve its resilience and maintain operational continuity. While no system is immune to attack, this strategy reduces vulnerabilities, supports regulatory compliance, and fosters a proactive security culture across the organisation.

# Recommendations

Collectively, the recommendations below help ensure that OURGAS aligns with the NIST framework and AESCSF, thereby ensuring an appropriate cyber defence plan is in place to mitigate incidents if they occur.

|  |  |
| --- | --- |
| **Product/Service** | **Approximate Price** |
| NGFWs: FortiGate and/or Cisco Firepower. | ~$100,000 - $250,000 initially, then $30,000 - $80,000 annually. |
| Ruggedised OT FWs: Fortinet Rugged and/or Cisco ISA. | ~$60,000 - $150,000 initially, then $15,000 - $40,000 annually. |
| 3-2-1 backup strategy. | ~$40,000 – $80,000 initially, then $10,000 – $25,000 annually. |
| Endpoint protection hardware: ruggedised and standard devices. | ~$300,000 - $450,000 for ruggedised devices.  ~$100,000 - $200,000 for standard devices. |
| SIEMs (threat intelligence, EDR, AV/anti-malware, patch management): Microsoft Sentinel, IBM QRadar, Splunk. | Microsoft Sentinel: ~$80,000 - $200,000 per year.  IBM QRadar: ~$200,000 - $500,000 per year.  Splunk: ~$150,000 - $400,000 per year. |
| Remote access using MFA and VPNs with IPSec (combining TLS, HTTPS, and SFTP protocols). | ~$40,000 - $100,000 initially, then $20,000 - $60,000 annually. |
| RBAC/ABAC systems: Azure AD, Okta, Ping Identity. | ~$20,000 - $50,000. |
| Security awareness training | ~$15,000. |

*Table 7: Recommended products and services*

# References

ACSC. (2023). *CYBER INCIDENT RESPONSE PLAN GUIDANCE*. <https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf>

AEMO. (2025). *AESCSF framework and resources*. Aemo.com.au. <https://www.aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources>

Amrez, Z. (2024). Endpoint Security: Threats, Defences and Best Practices [Review of Endpoint Security: Threats, Defences and Best Practices].

ASD. (2025, September). *Guidelines for cryptography*. Retrieved from <https://www.cyber.gov.au/business-and-government/cyber-security-frameworks/ism/cybersecurity-guidelines/guidelines-for-cryptography>

ASD. (2021, October). *Implementing network segmentation and segregation*. Retrieved from https://www.cyber.gov.au/business-government/protecting-devices-systems/hardening-systems-applications/network-hardening/implementing-network-segmentation-segregation https://www.cyber.gov.au/business-and-government/cyber-security-frameworks/ism/cybersecurity-guidelines/guidelines-for-cryptography

ASD. (2017, February). *Strategies to mitigate cybersecurity incidents*. Retrieved from https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/mitigating-cybersecurity-incidents/strategies-mitigate-cybersecurity-incidentshttps://www.cyber.gov.au/business-and-government/cyber-security-frameworks/ism/cybersecurity-guidelines/guidelines-for-cryptography

Barney, N. (2021). *What is a DMZ in Networking?* TechTarget. <https://www.techtarget.com/searchsecurity/definition/DMZ>

Canvas. (2024). *Fundamental Defensive Strategies and Considerations*. Usc.edu.au. <https://learn.usc.edu.au/courses/31755/pages/7-dot-2-fundamental-defensive-strategies-and-considerations?module_item_id=754113>

Cisco. (2025). *Cisco Firepower 1000 Series Firewall*. Cisco. <https://www.cisco.com/site/us/en/products/security/firewalls/firepower-1000-series/index.html>

Cloudflare. (2025a). What is a protocol? | Network protocol definition. *Cloudflare*. https://www.cloudflare.com/en-gb/learning/network-layer/what-is-a-protocol

Cloudflare. (2025b). What Is A Reverse Proxy? | Proxy Servers Explained | Cloudflare. *Cloudflare*. <https://www.cloudflare.com/learning/cdn/glossary/reverse-proxy/>

Fortinet. (2023). *Next-Generation Firewall (NGFW)*. Fortinet. <https://www.fortinet.com/products/next-generation-firewall>

Fortinet. (2025). *What Is Incident Response? Process & 6 Step Plan*. Fortinet. <https://www.fortinet.com/resources/cyberglossary/incident-response>

Fortinet. (2025). *What Is Network Security?* Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-network-security

Dolnicek, L. (2024). What Is A Bastion Host? Choosing A Network Security Solution For Your Business. *GoodAccess.* https://www.goodaccess.com/blog/what-is-a-bastion-host

Kamruzzaman, A., Ismat, S., Brickley, J. C., Liu, A., & Thakur, K. (2022, December 1). *A Comprehensive Review of Endpoint Security: Threats and Defenses*. IEEE Xplore. <https://doi.org/10.1109/ICCWS56285.2022.9998470>

OAIC. (2025). Notifiable Data Breaches Report: July to December 2024. Canberra: Australian Government. Retrieved from <https://www.oaic.gov.au/__data/assets/pdf_file/0021/251184/Notifiable-data-breaches-report-July-to-December-2024.pdf>

Microsoft. (2023). *About Azure Bastion*. Learn.microsoft.com. <https://learn.microsoft.com/en-us/azure/bastion/bastion-overview>

Microsoft. (2025). *What Is EDR? Endpoint Detection and Response | Microsoft Security*. Www.microsoft.com. <https://www.microsoft.com/en-us/security/business/security-101/what-is-edr-endpoint-detection-response>

NIST. (2024). The NIST cybersecurity framework (CSF) 2.0. *The NIST Cybersecurity Framework (CSF) 2.0*, *2.0*(29). <https://doi.org/10.6028/nist.cswp.29>

Palo Alto. (2015). *What is Endpoint Security Awareness Training?* Palo Alto Networks. <https://www.paloaltonetworks.co.uk/cyberpedia/endpoint-security-awareness-training>

Proofpoint. (2024). *Voice of the CISO.* Proofpoint.com. Retrieved from <https://nationalcioreview.com/wp-content/uploads/2024/06/pfpt-us-wp-voice-of-the-CISO-report.pdf>]

Pusin, Y. (2024, May 23). *The 3-2-1 Backup Strategy*. Backblaze Blog | Cloud Storage & Cloud Backup. <https://www.backblaze.com/blog/the-3-2-1-backup-strategy/>

Radware. (2024). *What is a Forward Proxy: A Comprehensive Guide | Radware*. Radware.com. <https://www.radware.com/cyberpedia/application-delivery/forward-proxy/>

SailPoint. (2023, September 7). RBAC vs ABAC: Definitions and differences. Retrieved from: <https://www.sailpoint.com/identity-library/rbac-vs-abac-whats-the-difference>

SAP Concur. (2025, March). *Business Expenses: Learn How to Manage Them Efficiently*. Retrieved from Concur.com: <https://www.concur.com/blog/article/how-to-efficiently-manage-business-expenses>

Widdowson, A. (2025a). Motivations and behaviour. In *Humans and Cyber Security: How Organisations Can Enhance Resilience Through Human Factors (1st ed.)* (pp. 16–35). Boca Raton: CRC Press. doi:10.1201/9781003427681-3

Widdowson, A. (2025b). Organisational vulnerabilities. In *Humans and Cyber Security: How Organisations Can Enhance Resilience Through Human Factors* (pp.59–73). Boca Raton: CRC Press. doi:10.1201/9781003427681-5

# Appendices

|  |  |  |  |
| --- | --- | --- | --- |
| **Meeting Date** | **Names** | **Decisions Made** | **Work Allocation** |
| 27/08/2025 | Torin  Kyle  Tereza | Work allocation regarding introduction and defence analysis headings. | Torin: Introduction and Endpoint Security.  Kyle: Data Security Protocols.  Tereza: Network Security Measures. |
| 03/09/2025 | Torin  Kyle  Tereza | Review work currently done and include the NIST structure to document. Allocating new sections to be completed before the meeting next week. | Torin: Endpoint Security and Human Factors.  Kyle: Human Factors.  Tereza: Network Security Measures and Respond & Recover. |
| 10/09/2025 | Torin  Kyle  Tereza | Reviewed completed work for the past week. Allocated ‘Respond & Recover’ subsections. Laid out a progression plan for the final week. | Torin: Response Planning, Recovery  Kyle: Communications, Analysis  Tereza: Mitigation & Containment, Improvements |
|  |  |  |  |

Table 8: Meetings

|  |  |  |
| --- | --- | --- |
| **Abbreviation** | **Full Term** | **Explanation** |
| ACSC | Australian Cyber Security Centre | Government body providing cybersecurity guidance, threat intelligence, and incident response support. |
| AES | Advanced Encryption Standard | A widely used symmetric encryption algorithm for securing sensitive data. |
| AESCSF | Australian Energy Sector Cyber Security Framework | A framework that helps energy organisations assess and improve their cybersecurity maturity. |
| AI | Artificial Intelligence | Technology that simulates human intelligence to analyse data, recognise patterns, and automate decisions. |
| APT | Advanced Persistent Threat | Advanced, targeted, long-term cyberattacks by state-sponsored or well-resourced groups to gain stealthy access for espionage, IP theft, or data exfiltration. |
| AV | Antivirus | Software that detects, prevents, and removes malicious software such as viruses and worms. |
| BYOD | Bring Your Own Device | A policy allowing employees to use personal devices for work often requires extra security controls. |
| CISO | Chief Information Security Officer | A senior executive responsible for an organisation’s information and cybersecurity strategy. |
| CSF | Cybersecurity Framework | A structured set of guidelines (e.g., NIST CSF) for managing and reducing cybersecurity risks. |
| DDoS | Distributed Denial of Service | An attack that floods a network or service with traffic to disrupt availability. |
| DMZ | Demilitarised Zone | A segregated network zone that hosts public-facing services to protect internal systems. |
| DNS | Domain Name System | Translates human-readable domain names (e.g., example.com) into IP addresses. |
| EDR | Endpoint Detection and Response | Tools that monitor, detect, and respond to threats on endpoint devices. |
| FTP | File Transfer Protocol | An older standard for transferring files over a network, now often replaced with secure alternatives. |
| HR | Human Resources | Department responsible for employee relations, training, and compliance. |
| HTTP | Hypertext Transfer Protocol | Protocol for transmitting data between web browsers and servers. |
| HTTPS | Hypertext Transfer Protocol Secure | An encrypted version of HTTP that secures web communications using TLS. |
| IDPS | Intrusion Detection and Prevention System | Monitors traffic for suspicious activity and can automatically block it. |
| IDS | Intrusion Detection System | Passively monitors network traffic to detect malicious activity. |
| IPS | Intrusion Prevention System | Actively blocks malicious traffic and attacks in real time. |
| IoC | Indicator of Compromise | Digital forensic data and observable artifacts from a network that indicate a security breach or cyberattack has occurred |
| IoT | Internet of Things | A network of connected devices that collect and share data. |
| IP | Internet Protocol | Core communication standard that routes data packets between computers and networks. |
| IPsec | Internet Protocol Security | A suite of protocols that encrypts and authenticates IP traffic. |
| IRP | Incident Response Plan | A documented set of procedures for detecting, responding to, and recovering from incidents. |
| IRT | Incident Response Team | A group designated to handle and mitigate cybersecurity incidents. |
| ISP | Internet Service Provider | A company that provides internet connectivity and related services. |
| IT | Information Technology | The use of systems, networks, and devices to process and manage information. |
| ML | Machine Learning | A subset of AI that enables systems to learn from data and improve over time. |
| MFA | Multi-Factor Authentication | A method requiring two or more forms of verification before granting access. |
| NAT | Network Address Translation | Modifies IP address information so multiple devices share one public IP. |
| NGFW | Next-Generation Firewall | An advanced firewall with deep packet inspection and intrusion prevention. |
| NIST | National Institute of Standards and Technology | U.S. agency that develops cybersecurity frameworks and standards. |
| OT | Operational Technology | Hardware and software used to monitor or control physical industrial processes. |
| PII | Personally Identifiable Information | Data that can identify an individual, such as names or ID numbers. |
| PLC | Programmable Logic Controller | An industrial computer used to control machines and processes. |
| PoLP | Principle of Least Privilege | Security concept where users get only the minimum access needed. |
| RBAC | Role-Based Access Control | Assigns user permissions based on predefined organisational roles. |
| RSA | Rivest–Shamir–Adleman | A widely used asymmetric encryption algorithm for secure data exchange. |
| SCADA | Supervisory Control and Data Acquisition | A control system used to monitor and manage industrial operations. |
| SIEM | Security Information and Event Management | Aggregates and analyses security logs and alerts across systems. |
| SFTP | Secure File Transfer Protocol | Secure version of FTP that encrypts file transfers using SSH. |
| SOCI act | Security of Critical Infrastructure Act | Regulation designed to protect key sectors from cyber-related threats in Australia. |
| SSL | Secure Sockets Layer | An older cryptographic protocol for securing communications, replaced by TLS. |
| TLS | Transport Layer Security | A modern cryptographic protocol that secures communications over the internet. |
| VPN | Virtual Private Network | Encrypts connections and allows secure remote access to networks. |
| WPA3 | Wi-Fi Protected Access 3 | The latest Wi-Fi security protocol with stronger encryption. |
| XSS | Cross-Site Scripting | A web vulnerability where attackers inject malicious scripts into websites. |

Table 9: Glossary of IT acronyms

# AI Acknowledgement

We acknowledge the use of Grammarly Premium for grammatical correction and sentence structure suggestions.