GOVERNMENT OF WESTERN AUSTRALIA

Office of Digital Government
Service Catalogue

June 2023

Produced and published by Department of the Premier and Cabinet
Office of Digital Government

Published June 2023

Principal address:
Dumas House
2 Havelock Street
West Perth WA 6005

Postal address:
Locked Bag 3001
West Perth WA 6872
Telephone: (08) 6552 5000
Fax: (08) 6552 5001

Email: dgov-administrator@dpc.wa.gov.au

Acknowledgment of country:
The Government of Western Australia acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures; and to Elders past, present and emerging.

Contents

Introduction

The Office of Digital Government (DGov) is an Office within the Department of the Premier and Cabinet, which leads, supports, and coordinates the digital transformation of the WA public sector.

Digital transformation is fundamental to a modern and effective public sector. Digital solutions enable WA Government agencies to change the way they work and reorient their services and processes around the needs of people and businesses – rather than the structures of government.

DGov works with WA Government agencies to support and accelerate their digital transformation journeys.

DGov leads and coordinates the implementation of the Digital Strategy for the Western Australian Government 2021-2025. The Digital Strategy puts people, businesses and communities at its centre and sets the vision for a public sector that leverages digital to deliver convenient, smart, and secure services for all Western Australians.

This Service Catalogue outlines DGov's current services available to WA Government agencies to assist with digital transformation and improve maturity, resiliency and data driven decisions.

The latest updated version of the Service Catalogue can be found online at wa.gov.au/DGovservices.

Guidance and Support

Digital Capability Fund Engagement

The Digital Capability Fund (the Fund) is administered by DGov. DGov collaborates with the Department of Treasury (Treasury) as appropriate.

DGov provides general advice on concept developments and informal feedback on draft proposals prior to being submitted to the Fund. DGov and Treasury jointly provide feedback to agencies on successful and/or unsuccessful proposals that were assessed through the Fund.

Service Type: On Demand

Time to commission service: Feedback or advise response times are dependent on resource availability and complexity of the query or submitted draft business case documents.

Methodology:

1. An agency that is developing a proposal that requests funding from the Fund, should inform themselves on the relevant policies and requirements by referring to the 'Important Links' below.
2. You may also reach out to DGov for the following:
    a. General advice on concept development.
    b. Informal feedback on draft proposals.
    c. Feedback on successful and/or unsuccessful proposals that were assessed through the Fund.
3. DGov reviews the draft business case, or any information provided and organises a meeting to provide verbal feedback and/or advice.
4. Where required, DGov may connect you with other units for further concept development assistance.

Outcome:

a. The proposal submitted to the Fund is in alignment with the Fund criteria and relevant whole of government policies.
b. The agency understands why they were unsuccessful and how to improve their submission for the next cycle, should they want to resubmit.

Benefit to the Agency:

The agency receives clear and tailored advice that addresses the Fund criteria and outlines any missing or incomplete information.

Important Links:

The Digital Capability Fund
Strategic Asset Management Framework

Contact details:

Info-dgov@dpc.wa.gov.au

Public Sector Digital Graduate Program

DGov administer the Public Sector Digital Graduate Program (the Program), which consists of two components, being a graduate program and a work integrated learning program. The Program will focus on in-demand ICT specialised areas, such as data science, cyber security, etc. Both components complement each other to create diverse and compelling opportunities for tertiary students and graduates, that leverages agencies' existing work streams, to create an attractive option for employment in the public sector.

Service Type: On Demand.
Time to commission service: Dependent on timing, applicants, and resources. Programs start once or twice per year.

Methodology:
1. An agency that wishes to participate in the program may reach out to DGov.
2. DGov will organise a meeting to understand the agencies requirements.
3. The agency will be invited to join the working group.
4. The agency will be required to formally commit to participating in the program, including creating and quarantining positions for any required graduates.
5. Graduates and interns will be assigned to participating agencies. Graduates will complete three four-month rotations; interns will complete 10-12 weeks placements.

Outcome:
Improved ICT skills and growth of digital capabilities across the public sector.

Benefit to the Agency:
This program provides the agency access to ICT graduates that can otherwise be difficult to attract. It also reduces the burden of managing and establishing their own internal graduate program.

Contact details:

digitalgradprogram@dpc.wa.gov.au

ICT Support Delivery

The ICT Support Delivery Team drives ICT program and project delivery across government, provides specialised technical skills and can help direct individual projects as needed. They have two primary functions:

1. Project co-delivery: Resources will be embedded in an agencies project team for a specific period of time to deliver critical stages of the project or for the life of the project.
2. Project assurance: Resources will be able to assist or direct projects that are off track either at agencies request or at the direction of the Minister for Innovation and the Digital Economy and/or the Digital Capability Fund Steering Committee.

Service Type: On Demand

Time to commission service: Dependent on complexity, priority and resource availability.

Methodology:

1. An agency may be allocated ICT resources to an initiative that:
    a. Has reported a red or amber status rating
    b. Has requested assistance to address any resource or skill shortage
    c. Is subject to ICT resource assistance as a condition for funding though the Fund
    d. Has a particular strategic importance or risk profile
2. DGov will organise a kick-off meeting between the agencies to determine roles, responsibilities and assistance requirements.
3. Upon completion of agreed resource allocation, DGov will reassess the agencies circumstances to determine if the time is to be extended or if the resource will return to DGov.
4. ICT resource to provide a summary report outlining:
    a. Timeline of events
    b. Results of engagement
    c. Findings and Recommendations
    d. Conclusion summary

Outcome:

1. The initiative will be reporting an improved status rating (either green or amber).
2. The agency will have received the ICT resource or skill required for the initiative.
3. The condition for funding has been met.

Benefit to the Agency:

- The Agency is provided with the resources and skills required to deliver programs and/or projects.
- The Agency has access to specialised ICT skills, which would otherwise be difficult to procure.

Contact details:

Info-dgov@dpc.wa.gov.au

Technical Platforms

ServiceWA App

The ServiceWA App (the App) allows users to access WA Government services in one convenient location. DGov is responsible for the App and the roadmap of services, and manages the onboarding of agency services into the App.

The App supports agencies to leverage the State Government's commitment to digital transformation and provide services to the public in one central location.

Service Type: On Demand

Time to commission service: As agreed during onboarding.

Methodology:
1. An agency may contact DGov to request a service be onboarded onto the App.
2. DGov will provide an onboarding pack which outlines the scoping process, responsibilities of both agencies and onboarding journey.
3. Where it is agreed to proceed, DGov will work with the agency to understand requirements including determining the funding required.
4. The onboarding process includes the following stages:
    a. Discovery
    b. Development
    c. Testing
    d. Pre-deployment
    e. Deployment
    f. Post-deployment
    g. On-going support (where required).

Outcome:
The Agency's service is offered through the App, providing another channel for individuals and businesses to access government services.

Benefits to the Agency:
a. The Agency has an additional avenue to deliver convenient and secure online services and information.
b. The Agency is not required to complete any App development procurement activities.
c. The Agency does not have to develop and manage their own App.
d. The Agency can increase savings and efficiencies by reducing duplication and use of more costly channels.
e. The Agency's customer can more easily find and access services through the whole of government App than through disparate websites and/or physical locations.

Important Links:
ServiceWA

Contact details:
support@digital.wa.gov.au

WA Digital ID Exchange

The WA Digital ID Exchange (WDIE) is an identity solution that will enable citizens to use a single identity to access many government services across WA agencies. There will be no need for citizens to remember multiple usernames and passwords for different online services and no need for agencies to build or maintain their own identity solutions.

Service Type: On Demand

Time to commission service: 3 months

Service Desk support: As agreed with onboarding service.

Methodology

Onboarding to the WA ID Exchange platform:

- Request use of service via an email to support@wa.gov.au
- Pre-engagement meeting to discuss agency's requirements, and platform offerings, and providing the relevant onboarding documentation to the agency.
- Sign a Memorandum of Understanding and Product Schedule committing agencies to use the platform.
- Agencies submit the onboarding documentation.
- DGov configure agency's environment to access WDIE.
- Agencies use the configurated link to either provide Digital Identity service or verify user's identity.
- A Service Desk is available to assist with additional queries from agencies.

Outcomes

- Agencies' digital services can utilise the WA ID Exchange to gain access to existing digital identity providers. This means the agencies no longer have to maintain their own usernames/password and that their customers can use the same Digital ID to log in to multiple agencies' digital solutions.

Benefits to the Agency

- Compliance with government digital standards and collaboration on digital maturity.
- Improved efficiency and lower operating cost and risk – no need to maintain expensive agency specific identity systems.
- Faster to deliver new digital services – you can quickly connect new digital services to the existing Digital ID Ecosystem.
- Uniform customer experience across agencies,
- Reduced risk of compromise to privacy data, since the agency no longer need to collect ID documents for identity proofing purposes.

Contact details:
support@wa.gov.au

Smart Form Platform

DGov recommends JotForm, a Software as a Service (SAAS) product as its Smart Form platform. JotForm is a sophisticated digital form platform designed for building online forms for WA.gov.au and other online applications. It offers an interactive page that emulates a paper document or form where users can fill out details including a combination of form elements such as a text boxes, checkbox, and a submit button.

DGov has an Enterprise Agreement with JotForm on behalf of WA Government that can be leveraged by agencies.

Service Type: On Demand

Time to commission service: Typically, available 1-2 weeks from request dependent on resource availability.

Service Desk support: Business hours

Methodology
To request access to the Smart Form platform:

- Reach out to support@wa.gov.au and request a quote.
- Sign a Memorandum of Understanding and Product Schedule committing agencies to use the Smart Form Platform.
- Once you've received a quote, respond, and approve quote in writing.
- Access is granted to the Smart Form platform.
- JotForm Service Desk is available to assist with additional queries from agencies.

Outcomes

- Allows for more sophisticated transactions online, enabling form owners to create and maintain forms conveniently without relying on technical resources.

Benefits to the Agency

- Easy to use.
- Security
- Low Cost
- Reliability / Reputation
- No minimum license requirements
- Leveraging the whole-of-government existing agreement with JotForm
- Easy cross-agency collaboration
- Access to exclusive ABN lookup widget
- Single-Sign-On (SSO) with Multi-Factor Authentication (MFA) in place with no additional cost
- Data centre in Sydney shared only with WA Government agencies subscribing through DGov.
- Free data collaborator account to access submission tables of each form

Contact details:
support@wa.gov.au

PeopleWA (Whole of Government Data Linkage Asset)

PeopleWA is a powerful new linked data asset that drives evidence-based medical research, policy development and government service improvement. It contains de-identified linked data about individuals' contact with services across government – including from the Departments of Communities, Education, Health, Justice (including the Registry of Births, Deaths and Marriages) and the Western Australia Police Force – to create richer, more comprehensive datasets.

The Department of Health (Health) undertakes data linkage for PeopleWA in a safe, privacy-preserving environment. DGov hosts linked data from participating agencies, coordinates applications for access to PeopleWA and provides access to data via a secure e-research platform.

Service Type: By application
Time to commission service: Dependent on the scope and complexity of applications

Methodology:

1. Agencies provide demographic data (identifiable data about individuals) to Health and content data (non-identifiable service data about individuals' interactions with government) to DGov. This is called the 'separation principle' and ensures that no party has access to both personal identifying information and content data, to protect individual privacy.
2. Department of Health undertakes data linkage and generates encrypted linkage keys utilising the demographic data. The keys are provided to DGov.
3. DGov integrates de-identified PeopleWA data utilising the encrypted linkage keys and agency content data identifiers.
4. Entities (government agencies, not-for-profit organisations, and researchers) seeking access to linked data in PeopleWA can apply to DGov, via the PeopleWA online application system.
5. DGov:
    a. Receives, reviews, and assesses applications for access to PeopleWA data;
    b. Works with applicants to refine applications, if required;
    c. Coordinates the review and approval of applications by relevant data custodians; and
    d. Provides access to de-identified data to Approved Users, in a highly secure e-research environment. Data cannot be removed from this environment.
6. Agencies that want to provide data to PeopleWA can fill in an 'additional datasets form' by contacting the PeopleWA team at peoplewa@dpc.wa.gov.au.

Outcome:
WA Government agencies, researchers and not-for-profit organisations can securely utilise rich, linked government datasets to inform and evaluate policy and investment decisions, and service delivery.

Benefit to the Agency:
PeopleWA data will support government and its stakeholders to tackle the most complex social, health, environmental and economic issues facing Western Australia in a more targeted and strategic way. Government agencies can utilise linked data to evaluate whether policies and programs are working, measure the effectiveness of preventative and early intervention strategies and target investment decisions.

Important Links:
PeopleWA

Contact details: peoplewa@dpc.wa.gov.au

WA.gov.au Content Management System (CMS) Platform

WA.gov.au is WA Government's central access point to whole-of-government citizen-focused digital services, bringing together WA Government information from various agencies into a single location, allowing citizens to easily find and access services.

WA.gov.au has been designed to meet universal accessibility standards, ensuring that everyone who needs the service can use it. The goal is to improve access to digital services for all Western Australians, including those with disabilities, living in remote areas, people with diverse cultural backgrounds and people using different devices such as smartphones.

Service Type: On Demand

Time to commission service: Typically, available 1-2 weeks from request dependent on resource availability

Service Desk support: Business hours

Methodology
Onboarding to the WA.gov.au CMS platform:

- Request use of service via an email to support@wa.gov.au
- Pre-engagement meeting to discuss offerings of the CMS platform and identify any additional requirements.
- Register for WA.gov.au CMS Training
- Sign a Memorandum of Understanding and Product Schedule committing agencies to use the platform.
- Agencies must ensure that their content complies with the Digital Service Policy Framework.
- Agency can commence transitioning relevant content to the CMS platform and publish at any time.
- A Service Desk is available to assist with additional queries from agencies, as well as granting users' access.

Outcomes

- Consistent user experience
- Mobile responsive design
- Focus on accessibility and inclusivity.
- Easier for consumers to find information and transact with Government based on a 'one Government' approach to service delivery and allows for better integration across government.

Benefits to the Agency

- Reduced ICT costs – savings generated by moving onto the WA.gov.au platform can be reinvested at the discretion of the agency.
- Reduced operational risks to the agency.
- Compliance with government digital standards and collaboration on digital maturity.

Important links: WA.go.au - Bringing the WA Government to you

Contact details:
support@wa.gov.au

Have Your Say

The ‘Have Your Say’ feature on WA.gov.au provides a central place for the public to find WA Government consultations that are happening across the state and offers opportunities for the public to share ideas and opinion on projects, services and government policy.

Service Type: On Demand

Time to commission service: 1-3 months

Cost of service: Varied depending on complexity.

Service Desk support: Business hours

Methodology

Onboarding to the Have Your Say platform:

- Request use of service via an email to support@wa.gov.au
- Pre-engagement meeting to discuss agency’s requirements, and platform offerings.
- Sign a Memorandum of Understanding and Product Schedule committing agencies to use the platform.
- Attend training.
- A Service Desk is available to assist with additional queries from agencies.

Outcomes

- Provide a central display for the citizen to view all current and past WA Government consultations.

Benefits to the Agency

- Consultations receive higher citizen exposure.

Benefits to the users

- Simpler to discover consultations that are relevant to them.

Contact details:
support@wa.gov.au

Web platform hosting-only service

DGov offers Amazon S3 (Simple Storage Service) Static Hosting solution for agencies requiring campaign or promotional websites, or agencies requiring a level of separation from Government, such as independent entities and statutory authorities.

Amazon S3 is a cloud-based storage service offered by Amazon Web Services (AWS). It provides a highly scalable and reliable platform for storing and retrieving any type of data.
S3 can be used to host static websites as well, meaning that you can use it to store and serve web content such as HTML, CSS, JavaScript, and images.

Overall, S3 hosting is a reliable, scalable, and cost-effective solution for hosting static websites and storing any type of data in the cloud.

Service Type: On Demand

Time to commission service: Typically, available 1-2 weeks from request dependent on resource availability

Service Desk support: Business hours

Methodology
To request S3 hosting:

- Request use of service via an email to support@wa.gov.au
- Pre-engagement meeting to discuss agency's requirements.
- Sign a Memorandum of Understanding and Product Schedule committing agencies to use the web platform hosting-only service.
- Provide a domain name at which you can use to view the hosting.
- Attend training on how to upload content to the S3 hosting.
- Agencies have the freedom to publish content on the S3 hosting whenever they want.
- A Service Desk is available to assist with additional queries from agencies.

Outcomes

- A highly scalable, available, cost-effective, and secure web hosting service for agencies.

Benefits to the Agency

- Reduced ICT costs – savings generated by using the web platform hosting-only service can be reinvested at the discretion of the agency.
- Reduced operational risks to the agency.
- Augment agency capability where it doesn't otherwise exist.

Important Link: Amazon Web Services CUAAWS2020

Contact details:
support@wa.gov.au

WA Domain Name Administration

DGov is the Domain Provider for the Western Australian Government and has the delegated authority to assess individual domain name applications for the WA Government.

The WA Government domain (. wa.gov.au) is reserved for use by entities within the WA Government.

DGov as the WA Domain Name Administrator (WA DNA) has responsibility for the following:

- Delegated authority for the wa.gov.au domain name registration and renewal.
- WA representative to the Federal Government Department of Finance's Government Domain Name Administration Team for all matters relating to Australian Government domain governance.

Service Type: On Demand

Time to commission service: Typically, available 1-2 weeks from request dependent on resource availability

Service Desk support: Business hours

Methodology

Two channels to seek assistance from WA Domain Name Administration Team:

- Complete the Apply for a new wa.gov.au domain name form on domainname.gov.au website; or
- Email your request to dna@wa.gov.au

Outcomes

- Compliance to WA Domain Name Standard, Australian Government Domain Name Policy, and Eligibility and Allocation Policy.
- Enforce the use of wa.gov.au in the Western Australian public sector.
- Reduce proliferation of domain names.
- More streamlined flow and coordinated approach in the governance and management of wa.gov.au domain.

Benefits to the Agency

- Support in obtaining and maintaining wa.gov.au domains for their websites, apps, and digital services.
- Conduit of receiving information and updates from Federal Government's Department of Finance's Government Domain Name Administration Team in relation to wa.gov.au domain and other relevant matters (such as corresponding .au domain name).
- Free service for agencies through centralised government funding.

Contact details:
dna@wa.gov.au

GovNext Management Service

DGov manage the GovNext Common Use Arrangement (CUA). This includes providing support and advisory services to agencies and managing the contractors.

GovNext has achieved its objective of moving State Government Agencies from purchasing ICT infrastructure to an ICT services consumption model. The GovNext contract term will expire in April 2024 and the Department of Finance is currently developing replacement buying arrangements.

Service Type: On Demand

Time to commission service: Typically, within 1 to 3 days.

Methodology:

1. An agency may contact DGov for assistance with:
    a. Buying services under the CUA
    b. Completing order forms
    c. Contractual questions and issues
    d. Order changes and extension of orders
    e. Exemptions and Policy Approvals
    f. Transition and decommissioning queries (to be moved to Department of Finance by midyear 2024).
2. DGov will create a new case in the Case Relationship Management (CRM) for the agencies query.
3. DGov will contact the agency either by email or phone. If required, a meeting may be organised to discuss the query in further detail.

Outcome:
The agency's query has been actioned and resolved.

Benefit to the Agency:
The Agency is informed on how to buy services through the CUA and how to use the order forms. There is also a reduced burden for the agency as the contractors and their contractual obligations, including insurance requirements, are managed by the Team.

Important Links:
GovNext ICT Products and Services Assist Cloud Transition

Contact details:
Govnext-dpc@dpc.wa.gov.au

Cyber Security

Overview

The Cyber Security Unit (CSU) within DGov leads, coordinates and supports whole-of-government cyber security efforts to protect the WA Government's information, assets, and service delivery from cyber threats.

This catalogue outlines the services aimed at improving cyber security maturity and resiliency to WA Government agencies. These services are offered **free** to WA Government agencies. Key areas of focus include:

- Security Guidance - Providing gap analyses on existing infrastructure and service design advice for proposed IT security systems.
- Essential 8 Maturity Improvements - Aiding in ACSC Essential 8 Maturity uplift at any level.
- Incident Detection Optimisation - Improve your Security Operations Centre connection and streamline your data logs for maximum threat detection without significantly increasing your subscription costs.
- Security Assurance - Perform security tests on proposed or implemented services or systems to identify vulnerabilities.
- Training and Awareness - Take advantage of our in-house expertise in cyber security training for all staff, including ICT specialists and executives.

Current programs of work to improve an agency's security maturity are grouped into two main areas - Capability and Uplift and Security Operations Centre services. A core tenet of the Cyber Security Unit is to identify vulnerabilities as well as offer bespoke assistance in designing and implementing changes for an agency.

Active Directory Password Review

An Active Directory (AD) password review involves retrieving password hashes stored and using tools which attempt to convert the passwords into plaintext format. This procedure identifies weak passwords which may be exploited through malicious attack which may lead to confidentiality, integrity and availability of the network being compromised.

Service Type: On Demand

Time to commission service: Typically, available 4-6 weeks from request dependent on resource availability

Methodology

The AD Password Review methodology includes:

- Pre-engagement meeting to define the scope activities and obtain permission to perform the password review.
- Extract the required files from the agency AD.
- Anonymise the account data and remove any personally identifiable attributes including usernames and Security Identifiers (SIDs)
- Crack the passwords by comparing them with a list of known password hashes and rulesets.
- Provide a report identifying vulnerabilities and provide mitigation strategies.
- Meet to discuss the mitigation strategies and further work.

Outcome

The final report will include the following:

- Summary of results
- Detailed findings and recommendations
- Analysis of user behaviour based on historic passwords cracked.
- Source and analysis files

Where necessary, additional information will be provided.

Benefits to the Agency

Password review seeks to provide the agency with the following benefits:

- Identify any weaknesses in the agency's current password policy.
- Identify commonly used and easily guessed password.
- Provide actionable suggestions to the agency.
- Encourage stronger authentication policy and practices.

Contact details: cybersecurity@dpc.wa.gov.au

Vulnerability Assessment

A vulnerability assessment (VA) identifies potential vulnerabilities within the scope of assessment. Identified vulnerabilities can potentially be exploited through a malicious attack, leading to degraded performance or a data breach. Detected vulnerabilities may be caused by poor configuration or a lack of regular software maintenance (patching).

Service Type: On Demand

Time to commission service: Typically, available 4-6 weeks from request dependent on resource availability

Methodology

The VA methodology includes:

- Pre-engagement meeting to discuss the scope, pre-requisites, and suitability of the project.
- Run the vulnerability scanner application including YARA rules for malicious file detection.
- Review findings and report results
- Exit meeting.

Outcomes

The outcomes of a vulnerability assessment include:

- Summary of results
- Assessment scope
- Assessment objectives and methodology
- Findings and recommendations

Benefits to the Agency

A VA seeks to provide the agency with the following benefits:

- Prevent data loss by identifying and addressing vulnerabilities.
- Inventory and audit devices to allow upgrades to be prioritised and identify assets needing further assessments.
- Provide tangible vulnerability and control effectiveness data allowing for a more informed approach to risk management.
- Identify areas of non-compliance with the Australian Cyber Security Centre (ACSC) Essential 8
- Identification of externally accessible devices and networks
- Identification of exposed confidential information
- Identification of login pages without multi-factor authentication

Contact details: cybersecurity@dpc.wa.gov.au

Vulnerability Management Review

The primary objective of implementing a vulnerability management process is to detect and remediate vulnerabilities in a timely manner. The purpose of this review is to improve the efficiency and effectivity of existing vulnerability management policy and processes in place.

Service Type: On Demand

Time to commission service: Typically, available 4-6 weeks from request dependent on resource availability

Methodology

The vulnerability management review methodology includes:

- Pre-engagement meeting to discuss the scope (including critical infrastructure) and pre-requisites and suitability of the project.
- Interviews with security personnel in charge of vulnerability management.
- Review of existing vulnerability scans.
- Support agencies in configuring the vulnerability scanner application to run YARA rules for malicious file detection.
- Review findings and report results.
- Exit meeting.

Outcome

The outcomes of a vulnerability management review include:

- Summary of results from interviews
- Summary of results from existing vulnerability scans
- List of externally exposed infrastructure and potentially sensitive data
- Findings and recommendations for vulnerability management practices

Benefits to the Agency

A vulnerability management review seeks to provide the agency with the following benefits:

- Defining or adjusting a well-defined process in place
- Assist in providing an agency with a continuous view of the risk associated with the presence of vulnerabilities existing.
- Identify critical infrastructure to be scanned regularly.
- Inventory and audit devices to allow upgrades to be prioritised and identify assets needing further assessments.
- Identify areas of non-compliance with the Australian Cyber Security Centre (ACSC) Essential 8

Contact details: cybersecurity@dpc.wa.gov.au

Active Directory Vulnerability Assessment

Active Directory (AD) plays an essential role in authenticating, managing, and granting permissions to users and devices on a network through a hierarchical structure. AD is the primary user directory and authentication provider in most Windows networks. If an attacker is able to gain access to the AD, they may be able to access sensitive information systems and information.

The AD VA will assess existing AD configuration to highlight insecure management practices and policy settings. Common issues include but are not limited to:

- Inappropriate management of accounts, privileged accounts, and security groups
- Inadequate policy restrictions
- Inappropriate infrastructure management
- Active legacy settings
- Improper configuration of settings and services

Service Type: On Demand

Time to commission service: Typically available 4-6 weeks from request dependent on resource availability

Methodology

The Active Directory VA methodology includes:

- Engagement meeting to discuss the scope and pre-requisites and suitability of the project
- Schedule an appropriate time to gather information identifying to identify weaknesses and misconfigurations
- Submit a report identifying vulnerabilities and provide mitigation strategies
- Exit meeting to discuss the findings and mitigation strategies

Outcome

The outcomes of an Active Directory VA include:

- Summary of results
- Detailed findings, analysis, and recommendations

Benefits to the Agency

Performing AD VA seeks to provide the agency with the following benefits:

- Identify weaknesses in user management policy and processes
- Identify conflicting policies leading to unexpected security settings
- Identify legacy settings which may leave the AD vulnerable
- Provide an overview of the AD structure and current state

Contact details: cybersecurity@dpc.wa.gov.au

Policy Mapping to Industry Standards

Policies are a vital part of an organisation as they provide guidelines to ensure that all information technology users adhere to the rules that apply within the organisation. Policy Mapping to industry standards will help align the agency's policy to industry good practice and identify gaps between the agency's current policies and the standards set by recognised organisations. It can also assist in identifying controls for inclusion in the Information Security Management System (ISMS).

The mapping process uses controls that are mentioned in several industry certifications/standards published by recognised organisations such as:

- International Standards Organisation (ISO27001)
- National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF)
- Australian Signal Directorate's Essential 8 (ASD E8)

Service Type: On Demand

Time to commission service: Typically, available 4-6 weeks from request dependent on resource availability

Methodology

The policy mapping methodology includes:

- Pre-engagement meeting to discuss the scope and pre-requisites and suitability of the project
- An evaluation of the agency's current policies
- Identify suitable controls from multiple certifications / standards published by recognised organisation
- Mapping of appropriate controls into the agency's policy
- Exit meeting to discuss the findings and mitigation strategies

Outcomes

The outcomes of policy mapping include:

- Summary of Results
- Assessment Scope and Methodology
- Assessment Objective and Findings

Benefits to the Agency

The outcomes of policy mapping include:

- Align an agency's policy to industrial good practices
- Identify gaps within the agency's policy
- Identify controls for inclusion in an ISMS

Contact details: cybersecurity@dpc.wa.gov.au

Australian Cyber Security Centre E8 Gap Analysis

The ACSC Essential Eight are technical security controls designed to quickly bolster agency networks against modern cyber threats. Agencies are required to report on the 8 controls and report on their implementation to DGov.

Service Target: On Demand

Time to commission service: Typically available 4-6 weeks from request dependent on resource availability

Methodology

The gap analysis methodology includes:

- An assessment of the design of an agency's current controls
- Identify gaps between the current state and the Essential Eight maturity levels
- Evaluate the effectiveness of current controls
- Outline controls that need to be in place to protect the agency's infrastructure
- Exit meeting to discuss the findings and mitigation strategies

Outcomes

The outcomes of an Essential Eight gap analysis include:

- Summary of results
- Assessment scope and methodology
- Assessment objective and findings
- Recommendations

Benefits to the Agency

An Essential Eight gap analysis seeks to provide the agency with the following benefits:

- Clarity of the current state of controls
- Identified areas of improvement to address risk
- Guidance for Essential Eight mandatory reporting

Contact details: cybersecurity@dpc.wa.gov.au

Security Design Review

The Security Design Review service aids agencies planning to implement new software solutions or platforms by evaluating security at various stages of the development lifecycle or deployment phases. Activities include threat modelling, identification of security requirements, and technical security solution design reviews.

Service Type: On Demand

Time to commission service: Typically available 2-4 weeks from request

Methodology

Security design review activities can be performed at various stages of a system's development lifecycle or deployment; from requirements gathering, solution and control design, development, implementation, and operation.

The exact approach to deliver these services will vary based on the engaging agency's internal cybersecurity knowledge, scope of the system being considered, lifecycle state of the system, and other factors. Commonly, the services are delivered through a combination of workshops and documentation review activities.

Outcomes

The outcomes of a security design review activity include:

- Identification of security threats
- Identification of security requirements
- Identifications of security deficiencies in solutions
- Recommendations regarding security considerations and requirements to be incorporated into the system
- Recommendations for security assurance activities to be performed in subsequent system development stages

Benefits to the Agency

Security design review services are primarily aimed at identifying security considerations and requirements in the earlier stages of a system's lifecycle. This allows the outputs of the review to inform the security capabilities to be built into the system.

Contact details: cybersecurity@dpc.wa.gov.au

Penetration Testing

Penetration testing is an authorised simulated cyberattack that identifies and exploits vulnerabilities of an application, service, or network to evaluate the effectiveness of security controls. A penetration test is an objective based assessment of an application, service or network intended to reach a particular goal through the discovery and exploitation of one or potentially a chain of vulnerabilities. Depending on the requirements of the agency, the service may include some aspects of vulnerability assessment (attempting to identify and qualify as many vulnerabilities as possible) or may be purely objective based.

Service Type: On Demand

Time to commission service: Typically, 4-6 weeks from request

Types of Testing

Penetration testing and the related services available across the team, including but not limited to:

- Web applications (including code assisted web applications) testing
- Mobile applications (and their web service backends) testing
- External and internal infrastructure testing (wired and wireless)
- Security Control validation
- Threat Detection validation
- Threat modelling

Based on agreement with the engaging agency, our approach to assessment typically employs either overt or attempted covert activities covering (where applicable):

- **Asset and service discovery** – organisations internal assets and services are enumerated to determine attack surface (identify live hosts, network mapping, port scanning, service fingerprinting).
- **Vulnerability scanning** – assets and services are scanned to identify vulnerabilities which can be exploited (common vulnerabilities such as poor patch levels and configuration issues).
- **Threat and Risk identification** – to systematically assess and analyse the potential vulnerabilities and threats that could impact the security of a system or network. By conducting a thorough evaluation, the goal is to identify and understand the various technical risks and threats that an organization may face.
- **User discovery** – enumerate valid user accounts, map the corporate active directory tree to identify targets.
- **Penetration exploitation** – exploitation of target vulnerable services or systems, verification of identified vulnerabilities.
- **Post exploitation** – valid account credentials, files are harvested from compromised system/s to demonstrate risk relevant to goals of penetration test.

- **Lateral movement** – compromised systems and accounts are used to compromise other systems on the target network.

Following the conclusion of testing, the findings and recommendations will be compiled into a report, with briefings as necessary. Retesting post remediation of any issues identified by the agency may also be performed.

Outcomes

The outcomes of a penetration testing activity include:

- Risk assessed summary of findings and recommendations.
- Details of the scope of the engagement and summary methodology
- Details of technical findings (typically including detail to the level where the issue can be replicated by the engaging agency) and recommendations for remediation.

Benefits to the Agency

A penetration test seeks to provide assurance of the sufficiency of technical security controls in place to prevent system compromise, and to provide advice to address areas of identified security risk exposure.

Contact details: cybersecurity@dpc.wa.gov.au

Training and Awareness Programs

The Cyber Security Unit offers training to agencies on topics including cyber security threats, cyber security policy, and hands-on activities designed to increase an agency's knowledge and expertise as part of their cyber security program. Programs can be tailored to an agency's specific requirements.

Live Cyber Security Awareness Training

This service offers comprehensive cyber security awareness training called 'Essentials' to all WA Government staff and external agencies. The training is designed to cater to different user groups, including Essentials Standard for all users, Essentials Plus for privileged users, and Essentials Premium for executive staff. The training aims to educate participants about cyber security and equip them with the necessary knowledge and skills to protect themselves and their organisations from cyber threats.

The training can be requested by agencies or attended ad-hoc by the general audience throughout the year. They will receive a post-session pack containing cyber hygiene checklists, tips for detecting phishing attempts, instructions on how to report threats/incidents, and additional resources to reinforce their learning and support their ongoing cyber security efforts. The agency training coordinator will also receive a training report, which provides an overview of registration, attendance records, insights from polls, and a post-training quiz.

Service Type: Live online or in-person tutorial

Service Duration: Approximately one hour

Time to commission service: 1-3 weeks from request depending on availability

Recommended participants: The cyber security awareness training is designed to benefit users at different levels, including Essentials Standard for all users, Essentials Plus for privileged users, and Essentials Premium for executive staff.

Outcomes and Benefits

Participants attending the cyber security awareness training will gain knowledge about various aspects of cyber security including:

- Cyber threats
- Best practices for data protection
- Identifying phishing attempts
- Reporting incidents

Attending this training will provide attendees with a baseline understanding of cyber security awareness aligned with DGov CSU's curriculum, and entities benefit from the acquired training insights.

Contact details: cybersecurity@dpc.wa.gov.au

Awareness Materials

DGov CSU offers a range of awareness materials which are designed to support cyber security awareness campaigns and reinforce consistent messaging within the agency. The materials include various resources such as posters, graphics, and guides, which are accessible online or via email.

Service Type: Digital Content

Service Duration: Instant

Time to commission service: 1-5 days, depending on availability of resources

Recommended participants: The awareness materials are recommended for all staff within the entity who are targeted for cyber security awareness campaigns. These materials can be customised to suit different roles, departments, or specific communication needs within the entity.

Outcomes and Benefits

Utilising the awareness materials provided by DGov CSU allows agencies to-

- Leverage pre-developed resources to reinforce consistent cyber security messaging to their staff
- Ensure a consistent and effective cyber security awareness campaign aligned with DGov CSU's communications
- Enhance the effectiveness of the agency's efforts in promoting a cyber security conscious culture among its staff

Contact details: cybersecurity@dpc.wa.gov.au

Community of Practice and Forums

DGov CSU operates the Cyber Security Working Group (CSWG), a Microsoft Teams forum designed to facilitate information sharing among entities. The CSWG serves as a community of practice for cyber professionals and leaders across WA Government agencies, providing regular updates and fostering knowledge sharing among its members.

Service Type: Online

Service Duration: Ongoing

Time to commission service: The lead time for becoming a member and accessing the CSWG resources will be communicated by DGov CSU upon inquiry.

Recommended participants: The CSWG is recommended for cyber professionals and leaders within WA Government who are interested in cyber security and information sharing.

Outcomes and Benefits

By becoming a member of the CSWG, entities can:

- Gain access to a community of practitioners who regularly share cyber security updates and relevant materials
- Attend scheduled meetings and informative sessions, participate in discussions in a dedicated Microsoft Teams channel and access member-only materials
- Use the group as a platform for networking, sharing best practices and stay updated on the latest trends and threats
- Enhance their cyber security capabilities and resilience

Contact details: cybersecurity@dpc.wa.gov.au

Phishing Simulation and Assessment

The last line of defence for an agency against an intrusion is the end user. It is important to train the user to detect and respond appropriately to various threats that they may face.

This service provides agencies with access to training and awareness content and testing methodologies to ensure continual improvement of the staff's awareness.

Service Type: On Demand Virtual/Online or In Person activity

Service Duration: 4-6 hours over 3-4 weeks.

Time to commission service: Available 4-6 weeks from request

Recommended participants: Security Managers/Security Operations

Outcomes

- Summary of results
- Training advice to address any issues identified in the simulation
- Potential capability to run phishing simulations in the future
- Findings and recommendations

Methodology

The methodology includes:

- Pre-engagement meeting to discuss the scope, pre-requisites, and suitability of the project
- Test the phishing simulation to check the various technical controls in place which may block the simulation
- Run the phishing simulation
- Provide a report on the overall performance and provide training content
- Support agencies in setting up their own infrastructure for future testing
- Exit meeting

Benefits to the Agency

A user awareness exercise seeks to provide the agency with the following benefits:

- Prevent data loss by assisting users in detecting potential social engineering attacks
- Provide the IT staff with tangible information to understand the risk of social engineering attacks in their environment
- Provides a methodology for continuous monitoring and improvement

Contact details: cybersecurity@dpc.wa.gov.au

Corporates Compromised (Executive Board Game)

The Executive boardgame is a discussion-based cyber security incident response exercise aimed at Agency Security Executives to assist agencies in testing and refining their incident response plans and procedures. Designed by the Cyber Security Cooperative Research Centre and hosted by DGov, Corporates Compromised is designed to align with the cyber security training and awareness outlined in the DGov Cyber Security Policy. The boardgame aims to simulate real-world scenarios and encourage Executives and Board members to discuss what would happen within their organisation if a cyber incident took place.

Service Type: On Request In-Person activity

Service Duration: 1-1.5 hours

Time to commission service: Available 2-5 weeks depending on availability

Recommended participants: Corporates Compromised is suited for executives and board members and can be played with up to 8 participants per board.

Outcomes and Benefits

The outcome of the boardgame is to provide an innovative and engaging cyber security training experience by leading participants through an interactive cyber-attack simulation.

By utilising a user-friendly physical board game as the centrepiece of the gamification experience, we aim to:

- Facilitate open discussions within an incident response situation
- Gain experience in quick decision-making within a cyber incident scenario
- Provide participants with a better understanding of cyber security applications

Through 'live' news reports and calls for responses, our goal is to create a fast-paced, fun, and memorable environment that introduces cyber security concepts into an organisation's security awareness training and complements routine computer-based education.

Contact details: cybersecurity@dpc.wa.gov.au

Incident Reporting Portal (IRP)

The cyber security incident reporting portal provides a secured login for the community to report cyber incidents and enable coordination of incident response activities.

Service Type: Ongoing

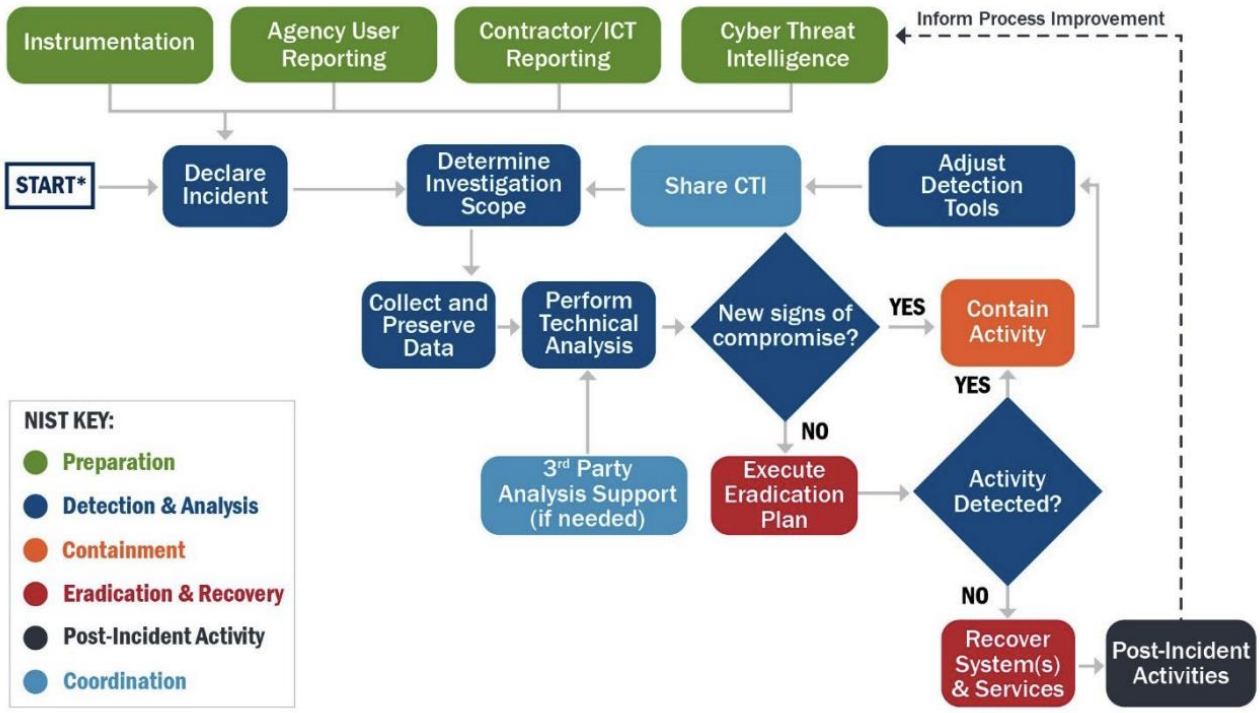
Time to commission service: On request

Service Target: See Critical Incident Response.

Agency Responsibilities: Report all known or suspected incidents within 24 hours. Review any WA SOC advisories and assess whether there is an impact to the Agency's systems and data in their custody.

Cyber Security Policy Areas: 4. Detect, 5. Respond

Methodology
Cyber incidents are classified and coordinated by the WA SOC under the WA CS Incident Coordination Framework and aligned to Information Technology Infrastructure Library (ITIL) practices. Incidents may be reported automatically (see Incident Triage Assistance) or manually. Agencies should refer to the CISA Incident Response Playbooks in the absence of an internal cyber incident management process.



Contact details: cybersecurity@dpc.wa.gov.au

Critical Incident Response

Cyber Security Incidents are managed under the WA CS Incident Coordination Framework. Agencies should ensure their cyber security incident response processes include appropriate detection, containment, and eradication procedures. The WA SOC recommends following the CISA Incident Response Playbooks in the absence of well tested, up to date agency specific playbooks.

Service Type: Ongoing

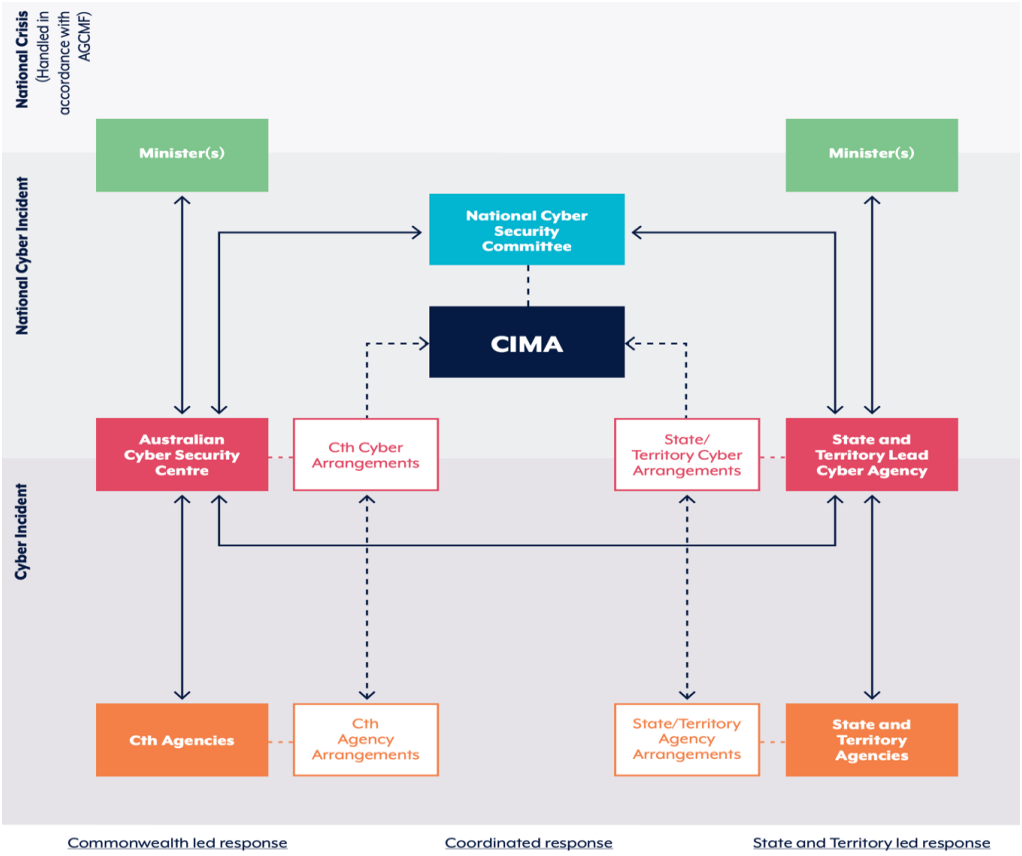
Time to commission service: On request

Service Target: Calls to 1800 922 923 (1800 WA CYBER) regarding Significant Cyber Incidents or Cyber Crises are responded to within 1 hour.

Agency Responsibilities: Ensure agency staff involved in cyber incident response are aware of the WA CS Incident Coordination Framework. Call the WA SOC and escalate relevant incidents within 24 hours of detection.

Cyber Security Policy Areas: 5. Respond

Methodology
The WA SOC will trigger critical incident response coordination activities using information recorded in the IRP, including WA Police and ACSC liaison where relevant. WA SOC resources will be allocated to response activities until risks reach an acceptable level.



Contact details: cybersecurity@dpc.wa.gov.au

Security Advisories

Publish timely security advisories using third party and internally-generated data sources and threat information. Note: Management of agency specific industry, legal, or regulatory sources are the responsibility of each agency.

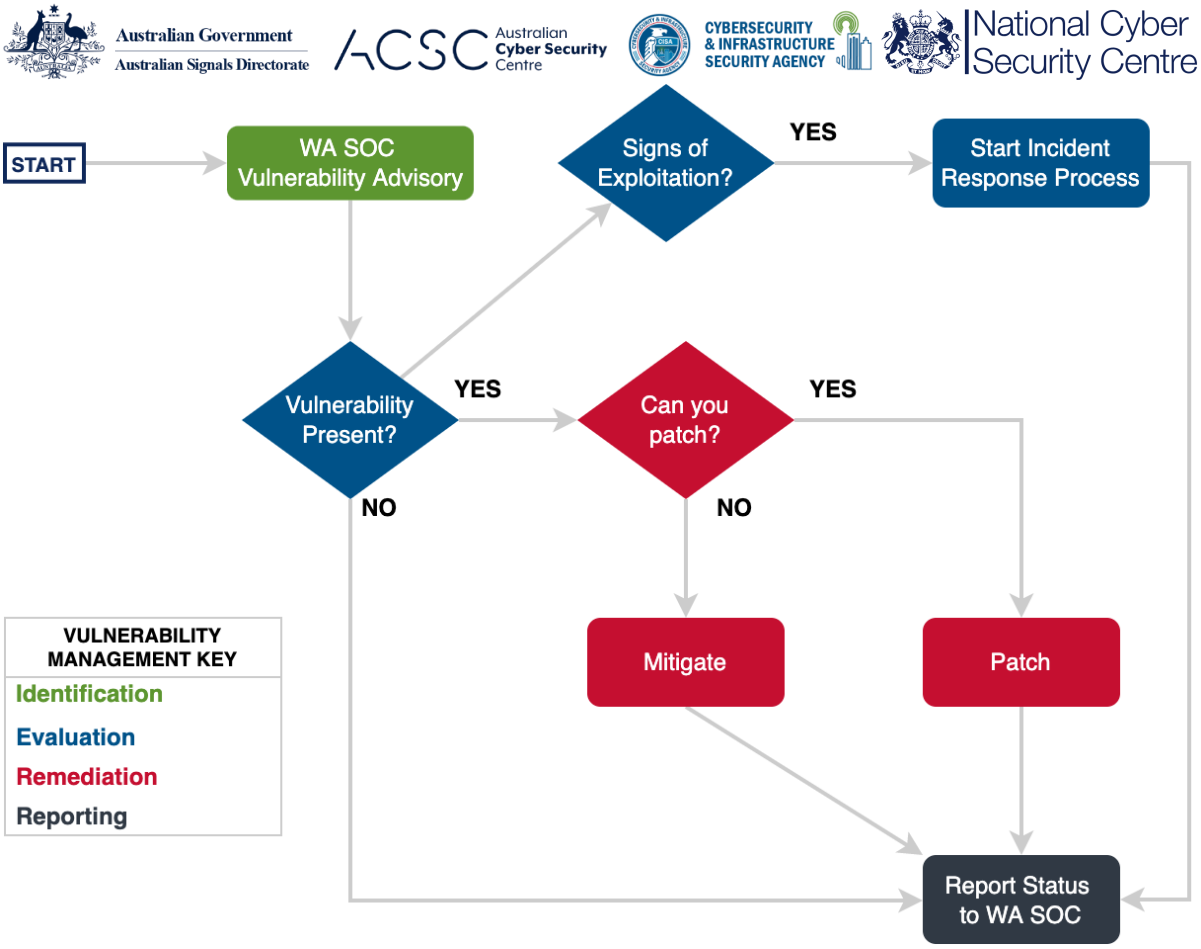
Service Type: Ongoing
Time to commission service: On request

Service Target: Advisories for CVSS v3 High and Critical (7.0 - 10.0) known exploited vulnerabilities distributed within 24 hours. Other advisories are reviewed for quality and accuracy and distributed within 1 week.

Agency Responsibilities: Provide email distribution list for delivery of advisories.

Wage Cyber Security Policy Areas: 2. Identify

Methodology
The WA SOC reviews cyber security advisories from Australian state and federal jurisdictions, ACSC, CISA, NCSC, private industry and internally generated intelligence derived from the WA SOC's threat hunting and incident monitoring activities. Agencies should refer to the CISA Vulnerability Response Playbooks in the absence of an internal vulnerability management process.



Contact details: cybersecurity@dpc.wa.gov.au

Automated Indicator Sharing

Automated Indicator Sharing (AIS) enables the exchange of cyber threat indicators across the community at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender's address of a phishing email. The goal is to ensure as soon as a stakeholder observes an attempted compromise, the cyber threat indicator of compromise (IOC) will be shared in real time with all partners, protecting everyone from that particular threat.

Service Type: Available on request

Time to commission service: On request

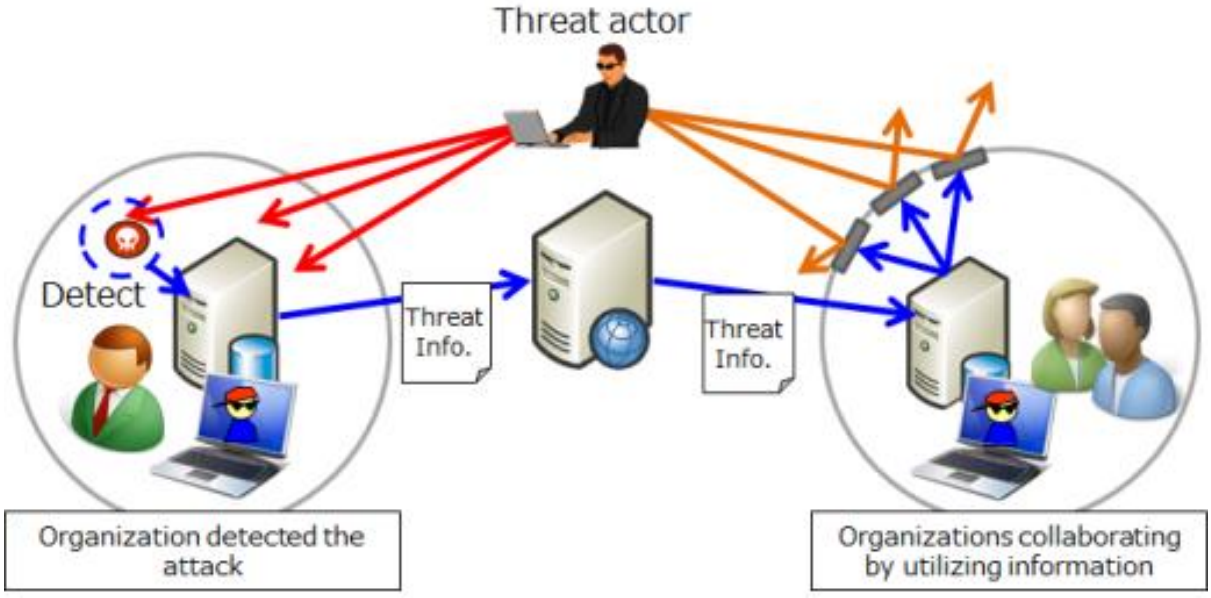
Service Target: TLP:WHITE or TLP:GREEN Cyber Threat Intelligence (CTI) collected during incident response is reviewed and published via WA SOC threat feeds within 4 hours.

Agency Responsibilities: Ensure requests for investigative activities during incident response are actioned in a timely manner, especially in situations where information may not be directly available to the WA SOC.

WAGov Cyber Security Policy Areas: 3. Protect, 4. Detect

Methodology

The WA SOC redistributes ACSC and select commercial CTI, as well as curates and distributes CTI specific to incidents it is coordinating. All incident derived CTI has its TLP level defined based on the source and is anonymised unless an agency requests to share its identity. CTI collected during incident response is collected in the WA SOC threat intelligence platform and made available via STIX/TAXII 2.0+. CTI may also be distributed via Security Advisories where broad community action is deemed appropriate due to the limited community consumption of automatically shared indicators.



Contact details: cybersecurity@dpc.wa.gov.au

SIEM Health Monitoring

Assessment of event ingestion and retention suitability across a given operational security environment. Actionable guidance to improve the organization's security environment, including specific recommendations, security best practices, and recommended tactical measures.

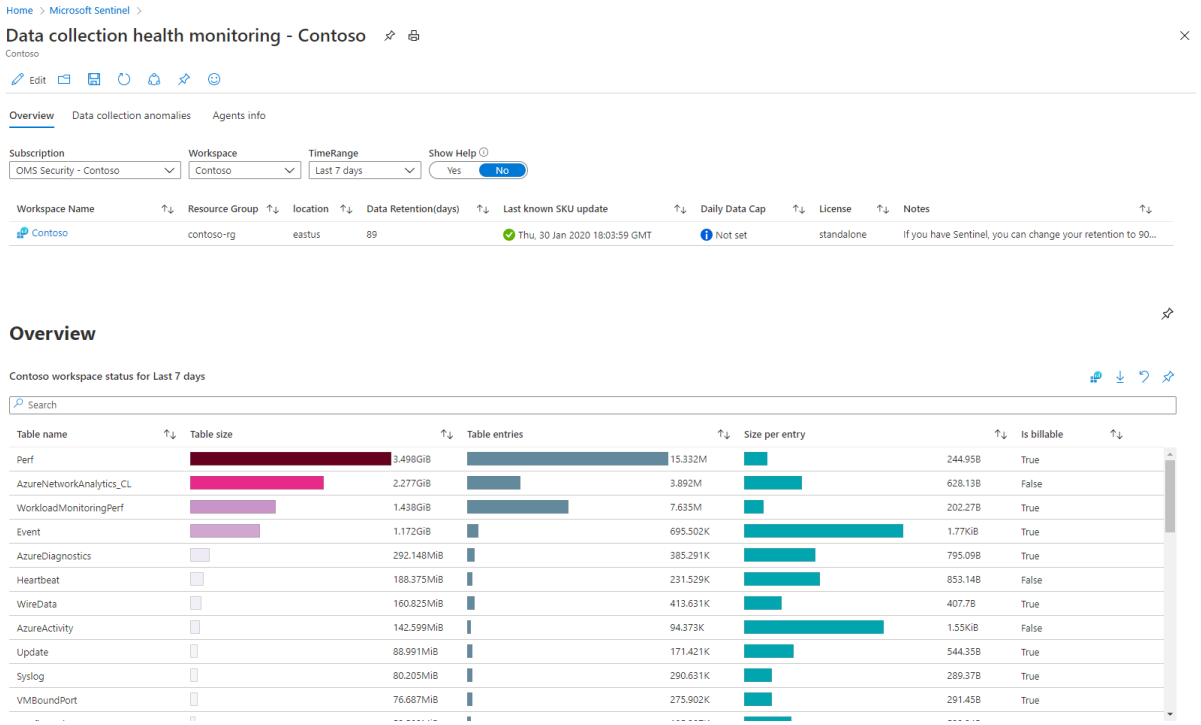
Service Type: Enabled once connectivity validated. Requires signing of MOU with Cyber Security Unit and onboarding to WASOC.
Time to commission service: N/A

Service Target: Security environment health overview focused on event data visibility and retention is included in monthly reporting.

Agency Responsibilities: Ensure the WA SOC is aware of the security environments in use, and has appropriate role-based access for automation accounts to query secured API endpoints for security event statistics.

WAGov Cyber Security Policy Areas: 3. Protect, 4. Detect

Methodology
The WA SOC queries event data daily using the Microsoft Sentinel API and Microsoft 365 Defender API where role based access has been delegated to WA SOC automation accounts. Aggregated statistics are persisted and used to generate monthly insights based on current best practices regarding event data collection and retention.



Contact details: cybersecurity@dpc.wa.gov.au

Incident Triage Assistance

Cyber Security Incidents are managed under the WA CS Incident Coordination Framework. The WA SOC provides ongoing liaison and support to agencies during the initial stages of triage from a potential detection, and where appropriate provides Critical Incident Response support for Significant Cyber Incidents and Cyber Crises. The assistance during triage is designed to ensure that agencies are able to rapidly classify and confirm the severity of incidents from all sources of detection.

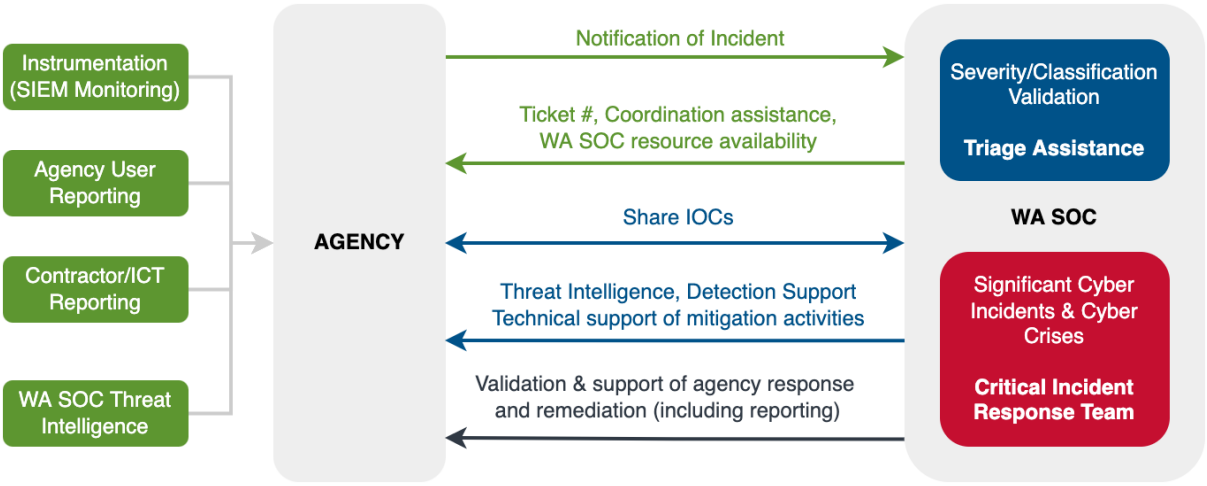
Service Type: Enabled once connectivity validated. Requires signing of MOU with Cyber Security Unit and onboarding to WASOC
Time to commission service: N/A

Service Target: WA SOC verifies agency incident triage for unresolved Medium and High severity incidents recorded in the IRP within 4 business hours (8am to 5pm excluding weekends and public holidays).

Agency Responsibilities: Ensure the WA SOC is aware of incident and problem management processes to interface with, and has appropriate role based access for automation accounts to query secured API endpoints for incident information.

WAGov Cyber Security Policy Areas: 4. Detect

Methodology
The WA SOC establishes integration services between agency Microsoft Sentinel environments and the Incident Reporting Portal (IRP). A queue of unresolved Medium and High severity incidents are analysed and understood. Subsequently incidents are then classified to determine appropriate further actions and priority status is assigned. Incidents are classified as either True Positive, Benign Positive, False Positive, and communicated back to the agencies existing incident and/or problem management processes.



Contact details: cybersecurity@dpc.wa.gov.au

Detection Analytics Health Monitoring

Reduce false positives, improve detections using formal CI processes and improve quality up the pyramid of pain. Monitor Automated Indicator Sharing and ensure high value indicators and tactics have appropriate detection analytics rules implemented.

Service Type: Enabled once connectivity validated. Requires signing of MOU with Cyber Security Unit and onboarding to WASOC

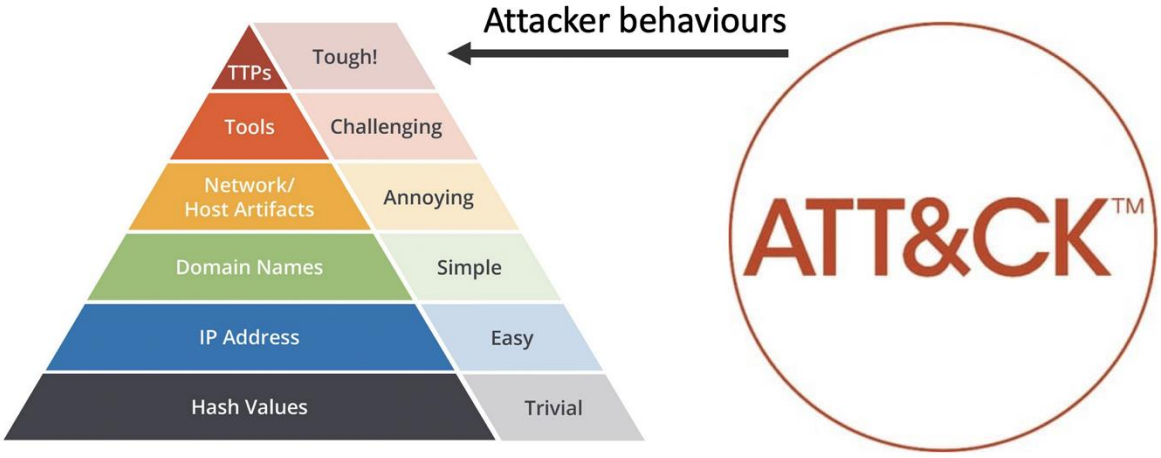
Time to commission service: N/A

Service Target: Security analytics health overview focused on detection analytics coverage and effectiveness is included in monthly reporting.

Agency Responsibilities: Ensure the WA SOC is aware of the security environments in use, and has appropriate role based access for automation accounts to query secured API endpoints for security events, detection rules and security incidents.

WAGov Cyber Security Policy Areas: 4. Detect

Methodology
The WA SOC queries information sources daily using the Microsoft Sentinel API and Microsoft 365 Defender API where role based access has been delegated to WA SOC automation accounts. Aggregated statistics are persisted and used to generate monthly insights based on coverage of MITRE ATT&CK® Tactics and detection effectiveness based on signal to noise ratios of analytics rules. Actionable guidance to address significant opportunities and risks is included in monthly reporting.



Contact details: cybersecurity@dpc.wa.gov.au

Detection Gap Analysis

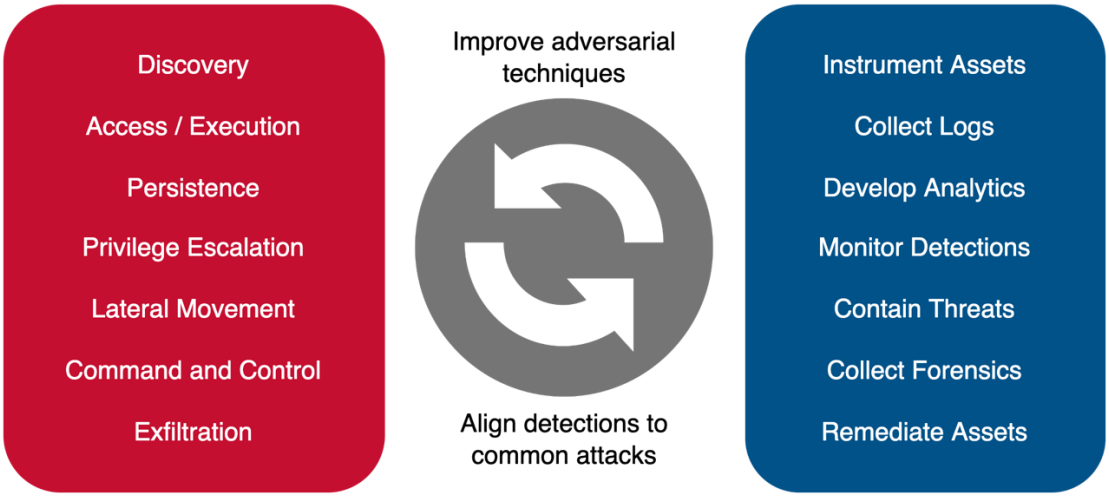
Work with agency resources in a joint exercise to conduct advanced tests of incident detection tools and responses using adversarial techniques.

Service Type: Available on request
Time to commission service: Typically, available 4-6 weeks from request dependent on resource availability

Agency Responsibilities: Work in collaboration with the CSU Capability and WA SOC teams to monitor testing activity and report events.

WAGov Cyber Security Policy Areas: 4. Detect, 5. Respond

Methodology
DGov CSU will identify appropriate targets with the agency, and review them for detection capabilities prior, during and after adversarial actions. Testing activities are undertaken in alignment with the MITRE ATT&CK® framework and provided as open information to the defensive team, to ensure that gaps in detection are reviewed and remediated throughout the engagement. This is an effective way to provide assurance and improve defensive capabilities against threat actors.



Contact details: cybersecurity@dpc.wa.gov.au

External Attack Surface Monitoring

Discovery of external facing assets (domains, IP addresses, certificates) including unauthenticated vulnerability scanning. Scan reports are included in the monthly vulnerability reporting from the WA SOC.

Service Type: Enabled once connectivity validated. Requires signing of MOU with Cyber Security Unit and onboarding to WASOC
Time to commission service: N/A

Service Target: External attack surface overview and trends are included in monthly reporting. Critical Incident Response triggered within 24 hours when high severity known exploited vulnerabilities are detected.

Agency Responsibilities: Ensure the WA SOC is aware of any changes to domain or IP address space ownership.

WAGov Cyber Security Policy Areas: 3. Protect.

Methodology
The WA SOC runs regular unauthenticated asset fingerprinting and discovery scans over each agency's external facing assets. This data is persisted and queried by Threat Hunting whole of sector scans to enable timely incident response. On request a comprehensive assessment and recommendations of actions to minimise an agencies exposure can be undertaken, see the Vulnerability Assessment service for more details.

Contact details: cybersecurity@dpc.wa.gov.au

Vulnerability Management

Vulnerability Management (VM) is a continuous, proactive and often automated process that keeps your endpoint devices – desktops, laptops, smartphones, tablets, servers, workstations, Internet-of-things (IoT) – safe from cyberattacks and data breaches. By identifying, assessing and accordingly addressing potential security weaknesses, agencies can help prevent attacks and minimise damage if a cyberattack does occur. The goal of VM is to minimise the risk exposure by mitigating as many vulnerabilities as possible.

The Office of Digital Government (DGov) is providing an opportunity for agencies to realise the benefits from having a centralised lens to vulnerabilities across agencies while reaping the rewards of the economies-of-scale. The current VM offering to agencies is free-of-charge and will include but it is not limited to:

- Performing a variety of scheduled Scans
    - Host Discovery Scans across the agencies internet facing devices
    - Vulnerability Scans
    - Web Application Scans
- Scanner Types - Cloud Scanners
- Credentialed Scans - Non-Credentialed Scans
    - Agents
- Executive Reporting of scan results using Lumin

In addition to the Vulnerability Scanning Services (VSS), the VM offering will assist agencies in complying with the Australian Signals Directorate (ASD's) Assessing Vulnerabilities and Applying Patches and will aid in the improvement of the agency's standing against the ASD's Essential Eight.

Service Type: Enabled once connectivity validated. **Time to commission service:** N/A

Service Target: Vulnerability overview and trends are included in monthly reporting. Critical Incident Response triggered within 24 hours when high severity known exploited vulnerabilities are detected.

Agency Responsibilities: Ensure the WA SOC is aware of the vulnerability data being collected, and has appropriate role based access for automation accounts to query secured API endpoints for vulnerability information.

WAGov Cyber Security Policy Areas: 3. Protect

Methodology

The WA SOC queries vulnerability data daily using the Microsoft Sentinel API and Microsoft 365 Defender API where role based access has been delegated to WA SOC automation accounts. Aggregated statistics are persisted and used to generate monthly insights based on current vulnerabilities and overall trend compared to the previous month. High severity known exploited vulnerabilities detection analytics are developed and included in Threat Hunting whole of sector scans to enable timely incident response.

To facilitate uptake of this service visit Vulnerability Scanning Service Description (www.wa.gov.au)

Threat Hunting

Provide scenario based threat hunting of security information to determine if an incident has occurred before detection. Results feed into the WA SOC's incident response process. Includes forensic examination of digital artifacts to detect malicious activity and develop further indicators.

Customised Hunting Activity

TTP Sweep and Protective Hunt- Available on request

Automated Threat Hunting

TTP Threat Hunt- Monthly Reporting

IOC Threat Hunt- Ad hoc

Time to commission service:

TTP Sweep and Protective Hunt- Typically available 4-6 weeks from request dependent on resource availability

TTP Threat Hunt- Monthly report, maximum 4 weeks from request

IOC Threat Hunt- Commissioned on an ad hoc basis based on threat intelligence

Agency Responsibilities: Provide security information on request to threat hunt team throughout an engagement.

TTP Hunt:

- Review the TTP Hunt results shared with you via email/JIRA ticket.
- Identify the detected TTP MITRE ATT&CK code and refer to ADS document.
- Understand the detection objectives and perform triage investigation against detected logs.
- Upon true-positive investigation results, raise an incident ticket with WA SOC. Reference: WA SOC - Incident Reporting
- Upon false-positive/benign true-positive investigation results, OR if you would like to request specific threat hunt TTPs, please contact cybersecurity@dpc.wa.gov.au

IOC Threat Hunt:

- Recommendations from any detections by the WASOC will be communicated directly with affected agency/agencies.

WA Gov Cyber Security Policy Areas: 2. Identify, 4. Detect

Methodology

The WA SOC undertakes lightweight ongoing threat monitoring as part of its Automated Indicator Sharing and Security Advisories services and extends this into in-depth targeted engagements to utilise common defender advantages over attackers. Preparation, modification of overall security controls and targeted detection/expulsion is the primary goal of targeted hunt activities, and feed into agency incident response and Critical Incident Response where appropriate.

Contact details: cybersecurity@dpc.wa.gov.au