consunet®

Trusted High-Assurance DevSecOps

Build the cyber and spectrum security future

Consunet

Consunet is a 100% Australian owned company that creates world-leading cyber and spectrum security technology solutions for Australia and its allies.

Based in Adelaide, a city of 1.4m and an Australian hub for Defence innovation, Consunet has more than 20 years of Commercial and Defence experience in high-assurance software and engineering.

Consunet operates from state-of-the-art secure facilities in the city's central business district, with capacity to expand within short time frames.

Australia's Defence and Intelligence communities entrust Consunet to design, develop, integrate, and sustain their operational capabilities.

- High growth Australian company employing over 100 highly skilled staff
- Dedicated in-house R&D team developing capability relevant intellectual property
- Proven ability to collaborate successfully with Defence, industry, and academia
- Rich experience includes partnering with Lockheed Martin, Royal Australian Air Force (RAAF), the Defence Science & Technology Group (DSTG) and the Trusted Autonomous Systems Defence Cooperative Research Centre (TASDCRC)

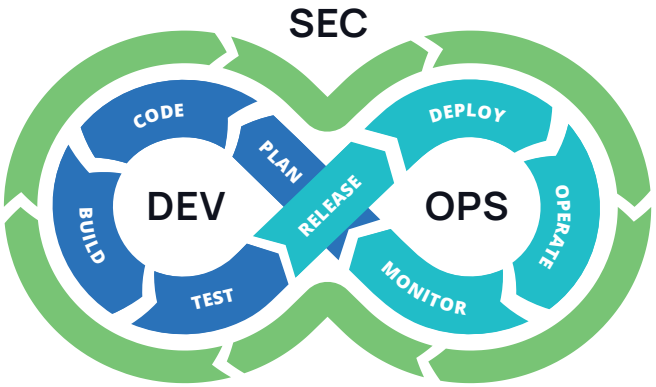
Understanding DevSecOps

DevSecOps is the concept of incorporating Security activities at every stage in the DevOps process. From planning, coding, building, and testing, to releasing, deploying, operating, and monitoring, Security is considered continuously. These stages are represented in the DevSecOps Infinity Loop. Applying security throughout the development process eliminates surprises, failed deployments, and most significantly—security breaches from threat attack vectors. DevSecOps reduces the likelihood of security being applied as an afterthought and provides opportunities to identify security issues upfront, reducing development costs and the potential for project overruns.

DevSecOps is achieved by ensuring security activities are the responsibility of both development and operations team members (both manual and automated) and includes security checks, code scanning, event monitoring, security controls and patterns/approaches to provide increased security. By embedding security into all phases of the development and operations processes, DevSecOps cultivates a business culture where development, security, and operations teams collaborate to maintain a secure, trustworthy, and speedy application delivery pipeline and operating environment, maximising uptime.

Challenges of Implementing DevSecOps
Despite its benefits, implementing DevSecOps can pose significant challenges for organisations and involves fundamentally shifting mindsets and processes. Successful implementation of DevSecOps requires an investment in training, tools, and education, to foster a continuous learning and improvement culture. Implementing DevSecOps requires a long-term commitment to security by all business teams.

Given the rising prevalence of cyber threats, this investment is not only valuable, but essential.



Trusted High-Assurance DevSecOps

The Consunet Capability Factory goes well beyond delivery excellence and lifecycle support. Alongside more traditional Continuous Integration/Continuous Development (CI/CD), we consider all the elements that will make your project a success on the ground, encompassing:

Consunet Capability Factory – the Elements

Product CI / CD Pipelines

- Strategic, multi-stage security controls
- Shared secure and trusted code and artifact repositories
- Repeatable, streamlined CI/CD pipelines

DevSecOps Services

- Proactive security monitoring with shared and common services
- Simplification and acceleration of development activities
- Developer support for effective collaboration within Agile delivery teams

Secure Infrastructure

- Store, host, process and access physical or virtual development / runtime environments
- Designed, built and accredited to comply with a variety of security classifications
- Increase trust in and assurance of your products and services
- Enable your delivery teams to focus on your customer and user needs

Collaborative Community

- Foster cohesion and collaboration, even within multi-vendor and supplier environments
- Deliver interoperable, flexible, trusted outcomes that consider ownership
- Embed collaborative thinking by deploying IP Frameworks and shared Code/Artifact repositories

Trusted Governance and Processes

- Ensure security processes are applied consistently, from planning, design, development and testing, through to deployment, operation and support
- Use/Apply DevSecOps for development and operations activities; IT Infrastructure Library (ITIL) for support activities
- Use hardened common infrastructure images; secure and regularly scanned repositories; and artifact containers with DevSecOps security and reporting services as part of Product CI/CD Pipelines
- Together these support the ongoing accreditation and authentication of the environment and products, contributing to increased trust levels

Open Architecture and Solutions

- Use Open-Source hardware and software interoperability standards, and open architectures based on componentised or service-based solutions
- Contribute to an environment and products that are transparent, secure, trusted and flexible, enough to support robust and emerging capabilities.

Consunet uses proven, robust solutions that have matured through the Cloud Native Computing Foundation (CNCF) and other US Government DevSecOps environments such as PlatformOne and their Customer DevSecOps Platform (DSOP) with elements such as the Iron Bank – DoD Centralised Artifacts Repository (DCAR) or the UK Defence DevSecOps Service (D2S).

Delivery High assurance trusted DevSecOps

To provide high assurance and trust, Consunet applies a maturity-based approach to DevSecOps CI/CD Pipeline design and implementation. Use of additional pre-flight actions, pre-scans, intermediary scans and monitoring solutions allow Consunet's customers to address concerns around supply chain attacks, hidden malicious code and libraries, code vulnerabilities and other risks that can affect the viability and trustworthiness of your products and services. Consunet's holistic approach increases your cyber fitness against attacks and provides proactive monitoring to identify and address risks, if they do occur, in a planned and controlled manner.

Pre-Flight

Use of
- Standardised hardened images
- Defined IP, licenses, common structures and best practices

To deliver baseline security, repeatable processes and practices.

Pre-Scan

Use of
- Secure scanned containers and source code
- Anti-virus scanning, vulnerability scans and code quality checks

To ensure quality and security for inputs into the environment and code.

Build & Test

Use of
- Automated unit tests
- Integration testing
- Contract tests
- Automation build and reporting

To ensure solution is regularly built and tested continuously to identify issues / bugs early.

Assemble

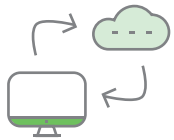
Use of
- Container builds
- Publishing artifacts
- OCI labelling
- Code and container signing

To ensure the solution packages correctly and are digitally signed.

Scan

Use of
- CVE scans
- Static code analysis
- Binary scans
- License scans
- Compliance scans (e.g. DISA STIG, ACSC ISM, ASD Essential 8, etc.)

To eliminate malware, vulnerabilities and security concerns.



Publish & Deploy

Use of
- Publish container
- Reporting pipeline performance
- Publish documentation
- Infrastructure automation (Ansible, Helm, K8s)

To ensure infrastructure & environment management and automation.

Observe

Use of
- Logging
- Monitoring
- Tracing

To ensure solution availability, performance management and capacity management. Support incident, problem, bug identification and remediation.

Are you SAFE?

50

Data Breach Notifications in 2022

Consunet has analysed Australian cyber breaches reported during 2022[1] and found several incidents targeting development environments with insufficient security controls and poor security practices. Crypto-style ransomware, which encrypts the organisation's data, appears to be on the decline. However, breaches of sensitive data stored and used within an organisation's test/development environments, are becoming more frequent. These are often caused by compromised user credentials, for example where developers and administrators have raised/modified access privileges, creating easier attack vectors for malicious actors.

0 1 1 0
1 0 0 1
1 0 1 0

Source Code Breached
Microsoft, Nvidia, Samsung, and LastPass were among the organisations that experienced data breaches where source code had been accessed. In many cases, this code was used as part of a ransom threat. However, more malicious entities use source code to identify other potential vulnerabilities in products, leading to future attacks with even greater impact. For example, Samsung's cyber threat actor could further compromise source code included in a company's secure applications and biometric operations.

Sensitive and Customer Data in Unsecured Development Environment
It was reported that both Optus and VinoMofo had data ex-filtrated due to lower security controls on test and development environments, which used live company or customer data. When working in any pre-production environment that uses live data (not recommended), the same rigor and security controls as the production environment must be in place.

Poor Security Practices
Multiple organisations reported breaches due to the use of weak credentials – including passwords such as 'Welcome1' or '123456'; or not handling credentials securely, for example storing in unsecured locations such as Personal Cloud File Storage. Good security practices must also be applied to development and pre-production environments.

Compromised User Credentials
Increased threats due to use of compromised user credentials are an increasing source of data breaches, either from Phishing attacks via email, phone or other communication platforms, through social engineering practices, or by using compromised data from a previous data breach. As above, security controls for your development environment should be as rigorous as controls in your primary production systems. This is even more important where developers have been granted higher administration rights for development and testing, because elevated rights in test environments can be used to launch wider attacks.

[1] Source: https://www.webberinsurance.com.au/data-breaches-list#twentytwo

Protecting Against Threats and Cyber Security Exploits

Consunet's services support your journey to achieving trusted, secure development practices. We offer turn-key engineering and DevSecOps environments to support new or migrated projects, and can uplift your existing project environments in situations where migration is less practical. Maturity assessments help you plan pragmatic strategic activities, while Consunet's advisory service provides a jump-start by identifying potential risks or roadblocks to your secure development capability through ongoing partnership arrangements. Consunet can design, build and maintain Managed Trusted DevSecOps Environments in the cloud, on-premise, hybrid or within classified enclaves. Consunet can deliver capability alongside existing teams or as a standalone service following Agile/systems engineering practices. These offerings support your strategic planning, risk mitigation, cost reduction, skill limitations and capacity needs to achieve a high assurance, secure and trusted development environment that customers and users demand in an increasing cyber threat environment.

Challenges

- Compare with peers
- Compromised libraries
- Customer cyber security demands
- Drowning in legacy
- Lack of trust
- No time for security
- Not sure where to start
- Unknown costs
- Unknown cyber risks
- Unmanaged risks
- Want to deliver faster
- What skills are needed

Maturity Assessments and Reviews

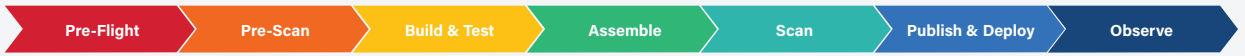
Identify vulnerabilities and security gaps to highlight actionable maturity improvements or good practices already in place. Articulate the target for a strong secure foundation to provide your customers and users the confidence, trust and assurance demanded in our cyber aware market. Consunet's discovery and review captures current and desired maturity levels to support a pragmatic plan for improvement.

DevSecOps Advisory and Guidance

Consunet DevSecOps experts provide guidance on best practices, lessons learned and implementation to support your achievement of Trusted DevSecOps Capability Factory outcomes for your business or customer applications. Advisory services can range from cyber security review through to design of rapid delivery in the most rigorous Defence or engineering heavy environments. Consunet can upskill your teams by providing access to skilled professionals to answer questions or provide guidance on complex or unique situations.

Managed Trusted DevSecOps Environments

Consunet can build new secure infrastructure or expand on an existing DevSecOps environment using cloud, on-premise or a mixture of both. This includes support, guidance and management to ensure efficient delivery, and ongoing security and maintenance of the environment.



DevSecOps and Engineering Delivery Services

Agile engineering services are delivered using Consunet's trusted DevSecOps CI/CD pipelines aligned with SAFe Agile and Systems Engineering processes and practices. Working as either a turnkey solution delivery team or in an integrated team alongside your own delivery teams. Consunet provides trusted, secure, quality solutions for your organisation and customers.

44 Waymouth Street
Adelaide, South Australia, 5000

GPO Box 449
Adelaide, South Australia, 5000

+61 8 8234 8819

contact@consunet.com.au

www.consunet.com.au