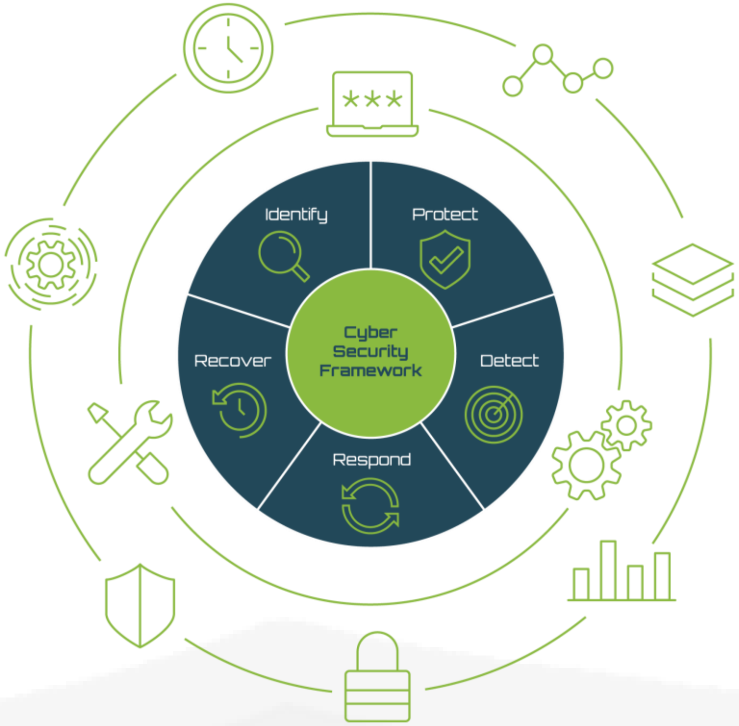
DEFEND Cybersecurity Management Services

ICE

Powered by DEFEND

Digital Transformation in Cybersecurity

- Organisations are continually evolving and changing to meet the demands of their customers and the business environment they operate in.
- The relentless drive to deliver digital services and modern workplaces means organisations must move faster than ever.
- This means that all parts of the organisation, including cybersecurity must be likewise transforming and enabling digital transformation.
- That requires understanding the changes in the threat landscape as the organisation evolves and providing the right strategies, services and controls to manage these threats.



At DEFEND we are committed to building partnerships with our customers to help them achieve a cyber enabled culture and improve their resilience. This means enabling them to move faster while providing the right level of cybersecurity to identify, protect, detect, respond and recover from threats.

New Zealand organisations are facing both technical and business challenges

31%

of organisations feel they have identified the parties that might attack their digital assets.

Source: Journey to Digital Trust 2019 PWC

Understanding the threat landscape

83%

of enterprise workloads will be in the cloud by 2020.

Source: Forbes 2019

Increasing move to the cloud

73%

of Nationally Significant Organisations in New Zealand increased their spending on cyber security in 2018. The NCSC concluded this had not increased confidence in organisations cyber resilience

Source: NCSC Cyber Security Resilience of Nationally Significant Organisations 2017 - 2018

Lack of confidence in investments

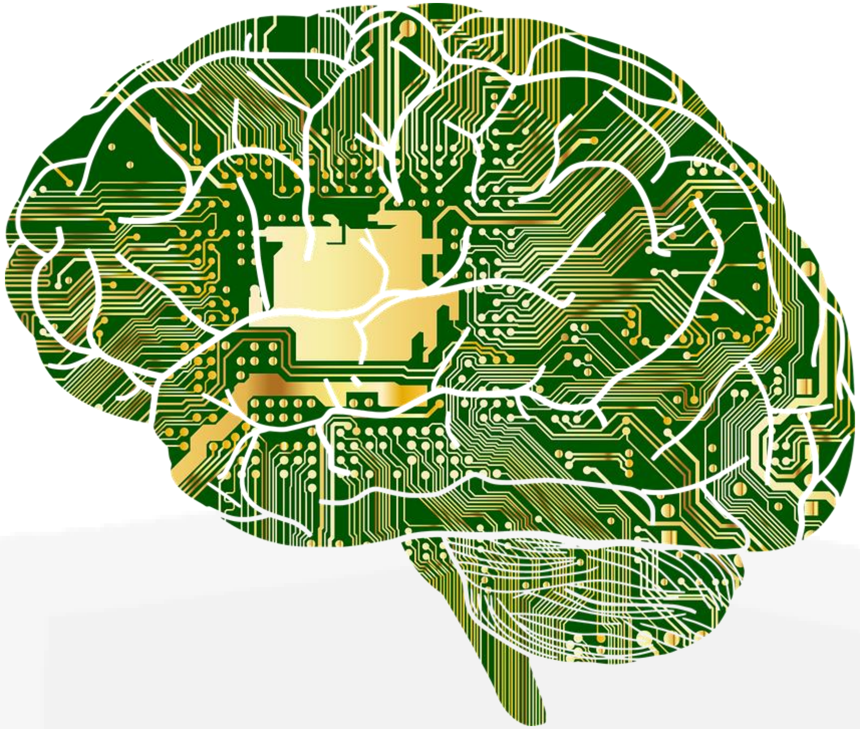
Cybersecurity Operations Evolution: The Shift Left Paradigm

- There must be shift left that ensures an integrated model that supports the organisation end to end.
- Cybersecurity operations is not a pillar outside of the organisation and cannot be limited to managing events and alerts.
- Without business context and awareness the required speed of identification, response, containment and recovery cannot be achieved.
- This needs to drive the natural evolution and increasing maturity of standardisation, optimisation and automation.

> “The traditional SOC and SIEM models are no longer effective and organisations need to embrace a shift left approach to standardization, automation and embedding cybersecurity within their lines of business.”
>
> Wenzel Huettner
>
> Chief Cybersecurity Architect
> DEFEND

DEFEND ICE - Intelligent Cybersecurity Ecosystem

DEFEND Intelligent Cybersecurity Ecosystem (ICE) delivers an end-to-end threat management capability that is integrated with the organisation and focused on protecting its digital assets. ICE provides a modular ecosystem that imbeds, complements and strengthens existing capabilities and delivers a decisive response to cybersecurity threats in real-time providing the right level of protection and response.



This service is delivered using DEFEND people, processes, and technologies that bring together our integrated ICE offering and delivers an automated intelligent platform that evolves with your business.

DEFEND has brought together leading experts from across NZ and around the world and combined their experience to develop and deliver a proven service which enables and delivers deep insights and automated response into cyber threats faced by organisations across New Zealand.

DEFEND ICE Architecture

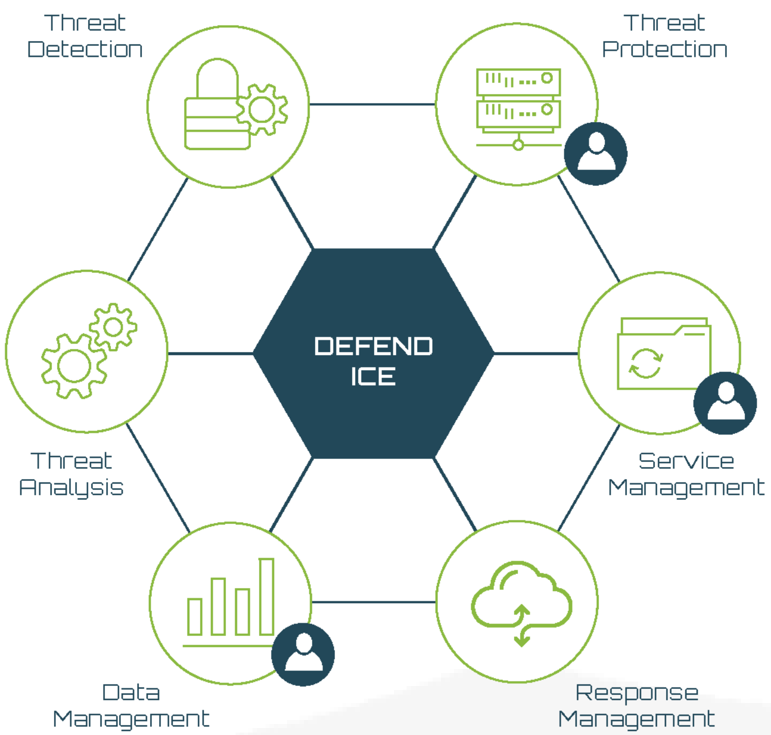
DEFEND ICE has been architected and built from the experience of delivering managed security services to some of New Zealand and Australia's largest organisations over 15 years. It has been designed and built with the understanding that:

- All organisations are slightly different and have their unique aspects;
- Security needs to cover the entire organisation and that there can't be any gaps, and
- Existing technology and service investments need to be integrated and cannot just be replaced.

All our service options can be connected with our *service nodes* to achieve the optimal outcome and can evolve and transform as your organisation changes and technology investments reach their lifecycle refresh.

DEFEND ICE Day One can be operating within 24 hours.

DEFEND ICE Nodes



DEFEND ICE Service Nodes

Threat Detection

Using our standardised framework and specialised threat intelligence network we create and monitor for a defined list of threat indicators that are collected either on day one or as part of a roadmap to build capability.

Service Options:

- **DEFEND Provided** – Utilising our threat detection tools and capabilities designed, implemented and lifecycle managed in your environment.
- **DEFEND Supporting** – Leveraging your capability and infrastructure with our support to ensure the right configuration and management.
- **Customer Managed** – We support you to put in place the right configurations on your infrastructure and systems.

Data Management

Data and log management are still important for defined correlations and allowing for both proactive and reactive analysis of trends or specific incidents. The important part if collecting the right data.

Service Options:

- **DEFEND Delivered** – We can provide our cloud based capabilities to collect datasets aligned to the defined threat use cases.
- **Customer Delivered** – We can assist with deploying or improving your cloud based or on premise capabilities be it Syslog, Elastic Search, AWS, Azure or any other technology platform.

DEFEND ICE Service Nodes

Threat Analysis

Key to DEFEND ICE is our expertise and experience in threat analysis and ensuring our unique *Event Analytics Framework* is implemented:

Service Options:

- **DEFEND Provided** – We can use our cloud based analysis platform leveraging a combination of Azure Sentinel, our AWS services and Sumo Logic as appropriate.
- **Hybrid Capability** – We can leverage existing SIEM solutions or analytics platforms and supplement with our framework and platform where required.
- **Customer Managed** – We can build out framework into most existing technologies and sometimes this is a good measure while we support you in building your improved capability or leveraging our platform.

Threat Protection

As environments mature we look to build automated and integrated response capabilities. This includes improved protection controls leveraging existing investments or improved capabilities aligned to the larger ecosystem.

Service Options:

- **DEFEND Managed** – We help to design, implement and/or manage a range or cloud or on-premise protection systems.
- **Customer Managed** – We can assist you in ensuring your systems are optimally managed and integrated into DEFEND ICE where possible to achieve optimal protective capability.

DEFEND ICE Service Nodes

Service Management
We have defined threat and event methodologies that are either mapped into customer systems or leverage our platform.
Service Options:

- **DEFEND Managed** – Provided by us using our people and either ServiceNow or Jira Service Desk
- Co-Managed – Leveraging customer teams and systems integrated with DEFEND people and systems
- **Customer Managed** – Customer provided system with integration to DEFEND ICE Response Management.

Response Management
Our specialised response teams provide continual support with rapid tiered escalation based on defined threat scenarios aligned to each of our customers.
Service Options:

- **DEFEND Managed** – Provided by us using our specialised teams and alerting tools (alerting, conferencing, communications, notifications).
- **Co-Managed** – Integrated with the our teams and leveraging a mix of our tools and customer based (e.g. conferencing/communication platforms).

Why DEFEND: Capacity & Capability

- **Focus** - We understand that cybersecurity services are not like managed services. All events and incidents must be considered positive until proven otherwise.
- **Expertise** - We have dedicated specialists who are appropriately trained and have the right tools for the job.
- **Experience –** This is what we do, we live and breathe cybersecurity every single day and all our teams have depth and capability spanning many years.
- **Integration –** We will not deliver a service that is lost in a team somewhere far away. Success must include integration and business understanding.
- **Mindset –** We are all trained to look at problems holistically, understand the business and provide the appropriate outcome.
- **Continuous Improvement –** Our services are designed to improve over time and drive cost savings and effectiveness through automation and customer uplift
- **Flexible –** We will adjust, flex and develop our capability to meet your business outcomes and enable your digital transformation.

DEFEND™