A SOC BUILT FOR YOUR NEEDS

SECURITY OPERATIONS CENTRE

infotrust

SECURING YOUR FUTURE.

SECURITY OPERATIONS CENTRE (SOC)

The proliferation of digital transformation along with the adoption of hybrid working has brought many benefits to organisations, but also greater risk. So much so, the need for expert eyes to monitor your environment for security vulnerabilities and threats, as well as recommend enhancements, has never been greater.

Managed detection and response, delivered through a security operations centre (SOC), is now considered a staple of any medium to large enterprise's security strategy. A SOC is a centralised unit that deals with security issues on an organisational and technical level, managing and enhancing an organisation's security posture. Crucially, it's people, processes and technology that help decipher what a great partner should provide.

Knowing Where to Start

With cyber security evolving so quickly, it can be hard to know exactly what your organisation needs from a SOC partner. To the untrained eye, the variety of SOCs on offer appear very similar. But dig beneath the surface to uncover the nuts and bolts, and the disparity between the average and the awesome becomes very apparent.

The Right SOC Investment for Your Organisation

Managing the right security posture for your organisation begins with listening to what you need. It's about trusted, expert advice based on years of experience, specialised resourcing through the very best people and implementation and management of the right capability to fit around your business.

Importantly, learnings and recommendations should feedback through to your organisation, helping you balance innovation and risk. Therefore, you need the very best people managing your SOC.

THE INFOTRUST SOC

The Infotrust SOC is where our highly skilled cyber security analysts use their specialised, deep expertise and highly developed processes to manage and enhance your security posture, through world-class technologies.

To deliver the right SOC, we must understand your organisation, risk profile and the outcomes you want to achieve. This ensures our deep expertise can build the right foundations for your SOC services and apply a level of customisation that fits your business, and your business alone. Forcing you to use certain platforms and SIEM - Security Information and Event Management technologies not in line with how your organisation operates results in poor agility. You need to be able to move quickly in the face of an increasing threat landscape.

Personalisation at the Core

The Infotrust SOC is built around three core foundation offerings and is designed as an extension of your team; no matter if you are a mid-sized organisation through to a large enterprise, but importantly based upon your own specific security requirements. We've got you covered across security incident management, managed SIEM and extended detection and response (XDR). You can also choose your desired service levels, as well on or offshore preferences.

Managed Detection and Response Foundation SOC Service

Custom Solutions for Enterprise & Government

Managed security services delivered from a highly specialised Security Operations Centre with technology of choice and XDR options. The synergy of incident response, threat intelligence, vulnerability management and security operations.

What's Included:

Solution tiers based on technology coverage, service levels and team locations with enhancement offerings.

Extended Detection and Response (XDR)

- Enhance your SOC with data correlation across multiple security layers
- Extend detections by integrating endpoint, server, network, data and cloud security.

Security Information and Event Management (SIEM)

- Maintenance and upgrades
- Detection and log source development
- Splunk, Microsoft, Sentinel, Rapid7 Insight

Security Incident Management

- SIEM monitoring and triage
- Investigation and notification
- Escalation evaluation guidance

Moving beyond our foundational solutions, we have a whole host of managed service extensions to enhance your Infotrust SOC, which we can implement based upon your needs and what you want to achieve. These include and are not limited to, cyber threat intelligence services and managed endpoint security, through to managed cloud security and email gateway filtering.

Choose from a range of solutions to form your own personal Infotrust SOC:

Essential

Essential SOC services to manage your security posture, triage threats, and notify your internal teams. Benefit from activating existing cloud security capability without or with low cost technology uplift.

Professional

More complete SOC capability beyond the SIEM, spectrum of XDR integrations, may include pro-active security activities.

Enterprise

Highly customised SOC services, fully developed security stack integrations, mature SIEM deployment, threat hunting and full service incident response.

Service Level

- Business Hours
- 24/7

Location Based

- Global including Australia
- Australia Only

With foundational services in place and we recommend SOC enhancements best suited to your business' needs.

Cyber Threat Intelligence

Intelligence Services

- Threat Intelligence Platform integration with SIEM
- Threat reporting powered by curators
- Dark/Deep Web detection and response

Vulnerability Management

VMaaS

- Risk-based patch management
- Asset ID, Scan, Report
- Prioritisation and Testing

Security Operations

Cloud Security

- Cloud access security broker tuning and management
- Secure Services Edge (SSE)

Data Security

- Data and file security monitoring and tuning
- Insider threat mitigation

Proactive Security

- Threat Hunting
- Testing & Red Teaming
- Phishing awareness

Endpoint

- Endpoint Detection and Response (EDR) tuning, policy enforcements and maintenance

Email Gateway

- Suspicious email investigations
- Email filter tuning

A CULTURE OF CONTINUOUS IMPROVEMENT

While a SOC is built around ensuring risk mitigation, it's also much more than that. Infotrust SOC is about ensuring constant refinement of your security posture to deliver continuous improvement.

Through our expert people and processes, we reach back into your business to help you consider architectural, platform or system changes that help reduce your attack surface and manage vulnerabilities. This delivers the outcomes and efficiencies your organisation should realise from a SOC investment.

Take for example our 24/7 monitoring capability. Threat actors don't discriminate based on the time of day. Capturing a threat in its tracks at 3am, as opposed to picking it up at 8am when other SOC teams arrive for work will have huge implications in preventing reputational or financial damage to your business. The details matter.

The Right SOC Investment for Your Organisation

Managing the right security posture for your organisation begins with listening to what you need. It's about trusted, expert advice based on years of experience, specialised resourcing through the very best people and implementation and management of the right capability to fit around your business.

Importantly, learnings and recommendations should feedback through to your organisation, helping you balance innovation and risk. Therefore, you need the very best people managing your SOC.

Focus on your core business

Trust our cyber security specialists and deep technical expertise, so you can focus on your core business.

Safety and resilience

We'll keep your business safe and help you build resilience to sustained cyber threats.

Custom-made for your organisation

We'll keep your business safe and help you build resilience to sustained cyber threats.

Maximise your investment

Ownership is retainer by your organisation to ensure you maximise your Infotrust SOC investment.