SECURITY OPERATIONS CENTRE

As an Australian cyber security vendor, NST has created an easy-to-implement solution focused on the needs of Australian Organisations. Our platform will enable you to enhance your cyber security detection and response capabilities without conducting expensive staff training or investing in long-term implementaion projects.

While most security solutions try to solve the threat detection problem from a particular angle, implementing detection capabilities either at the network, cloud, endpoint, or perimeter level, our platform embraces all your security data, from any environment: cloud, SaaS, network, on-premises, remote, or virtual.

NST provides a fully managed, plug & play experience, transforming machine data into actionable insights and executive-friendly reports. You do not need to maintain multiple security tools and run complex investigations with endless cross-system integrations, as NST establishes context for all security events in your organisation, automatically correlating data from multiple sources.

It takes minutes to deploy our cloud, network and end-point sensors which will feed your security data into our cloud platform hosted in Sydney, Australia. We offer a 30-day free trial with full access to all features - you can start now and see your data coming into the platform, in real time.

Integrate
Integrate your security data sources into the NST cloud platform in minutes; all data is hosted in Australia.
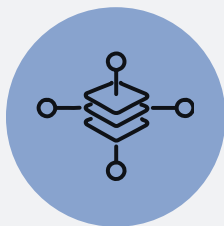
Training
Receive detailed onboarding training & onboarding training session for your IT team; your IT system administrators will become experienced security analysts over time.
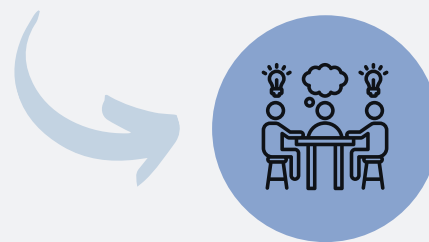
Compliance
Comply with ISO27001 and NSW Government Cyber Security Policy for detection and response capabilities, support Australian owned and made cyber security business.

Assessment & Report
Get your security controls assessment & report in real time, including Essential Eight maturity levels. Get immediate on-premises systems, Office365 and Azure AD.

Monthly Workshop
Receive a complimentary monthly meeting to get expert advice on your security posture, cyber risks, preventive technologies, etc.

Security Operations Centre - Highlights

NST delivers continuous assurance across all your cyber security functions and enables your security operations with rich threat context and unbeatable visibility across endpoints, servers, cloud, and SaaS applications. Paid with our 24x7 SOC as a Service, proactive Threat Hunting, and incident Response services, NST delivers unprecedented value to organisations of any size.

SEE BEYOND the limitations of your current security tools.
BE ABLE to answer any questions about your environment and report on anything.
MANAGE RISKS with third-party cyber risk protection.
PREVENT BREACHES with continuous vulnerability management and device hardening.
BLOCK ATTACKS with automated response capability and incident playbooks.
DETECT THREATS with automated detection and threat hunting.
PREDICT COMPROMISES with Dark Web monitoring and digital brand protection.
RESPONSE TO INCIDENTS with 24x7 SOC and proactive incident response.

HOW WE CAN ASSIST

Our solution offering is scalable to your requirement. We can provide a range of products that can be managed in-house with minimal training, offer ad-hoc professional services or entirely manage ongoing cyber assurance for your organisation. Our 24x7 team availability and intelligent sensors/tools assures your environment's security and integrity. In a worst case scenario, we are able to respond and contain risks rapidly while working with an existing ICT team.

You will be able to deploy professional SOC and SIEM services in one day, meeting all your compliance obligations and recording and storing logs from all your systems. In addition to this, you will get vulnerability management, Dark Web monitoring, integrated threat intelligence, security posture management for your cloud accounts, and many other features delivered to you as an integrated solution.

The platform will provide valuable insights from day one, and was used on multiple occasions in government organisations to reveal;

1. **Compromised legacy workstations used by hackers on your network**
2. **Compromised Office 365 accounts**
3. **Unexpected software**
4. **Exposed and vulnerable systems**
5. **Files with passwords in plain text stored by your users**
6. **Insecure external connections**
7. **User accounts targeted by hackers, and many other exposures and risks**

Our platform is delivered as a fully managed service, and our team will look after you. In addition to automated 24x7 alerting, our experts will conduct weekly in-depth security reviews (threat hunting) and will report on any unexpected events and other anomalies. We also will host a monthly review & training session, reviewing your cyber risks from the operational perspective and providing our recommendations.

WE BECOME PART OF YOUR TEAM

Our platform provides full enterprise coverage, integrating all the security data you can possibly reach into, including data that directly resides within your network and on your endpoints, as well as external data such as cloud workloads, SaaS applications, Dark Web breaches, compromised credentials, external vulnerabilities, and weaknesses and exposures related to third-party organisations in your supply chain.

Our Managed Detection and Response (MDR) get real-time threat detection, 24/7 threat hunting, thorough investigations, and full incident response lifecycle support. We pair our threat detection technology with trained and experienced security specialists who work 24x7x365 to deliver true cyber resilience capability to your business. Our Security Operations team detects, and analyses attack patterns and alerts your team as soon as possible. We will completely integrate into your current workflows and will follow your escalation procedures so you can counter a security threat before it causes any damage. Our focus is not on raising alerts, but on delivering great security outcome and defending your business from disruptions and data breaches.

ACSC ESSENTIAL EIGHT REPORTING

Our Customer Portal provides ongoing reporting, delivering a snapshot of your security posture in real time. We have hundreds of security metrics in our platform, and we can report on any of them. Our reporting covers security posture overview, ongoing operational issues, security trends over time, as well as various compliance frameworks such as ISO27001 and ACSC Essential Eight.

sales@nst.com.au | www.nst.com.au

BUSINESS CASE FOR YOUR CYBER DETECTION AND RESPONSE

Our platform provides unmatched capability to visualise your networks and systems and expose high-risk areas across cloud, on-premises, or virtual and delivers an end to-end cyber security solution, with full cycle detection, investigation, and response across all areas of your enterprise.

In addition to continuous, context-rich detection and response, our platform brings a real-time security assurance capability to your organisation. It provides ongoing monitoring of security configurations on-premises and in cloud, as well as detection of vulnerabilities and weaknesses in your external perimeter and your partner organisations to give important context and help predict external threats before they get a chance to reach your environment.

MIGRATE YOUR RESOURCE CONSTRAINTS:

	Cyber Essentials	24x7 SOC
Modern technology provisioning (SIEM, threat hunting)	✓	✓
End-to-end onboarding support	✓	✓
SaaS delivery model	✓	✓
Ongoing platform management	✓	✓
Log management	✓	✓
SIEM, detection rules and correlations	✓	✓
Vulnerability management	✓	✓
Dark Web monitoring	✓	✓
Email monitoring	✓	✓
Endpoint visibility and threat detection	✓	✓
Cloud monitoring (AWS, Azure, GCP)	✓	✓
Network and syslog monitoring	✓	✓
Application monitoring	✓	✓
24x7 alerts	✓	✓
Monthly security review	✓	✓
Weekly/monthly reporting	✓	✓
Essential Eight reporting	✓	✓
24x7 Eyes-on-Glass SOC		✓
Threat hunting		✓
Proactive Incident Response		✓