\Orchestrating a brighter world

Security Monitoring & Response

Security Information and Event Management

au.nec.com

Local capability
National capacity
Global coverage

Background

The explosive growth of smart technologies and connected devices that make up the Internet of Things (IoT) has resulted in a rapidly evolving threat landscape where attack types are changing constantly. Organisations require a range of mitigation strategies to effectively protect digital assets and meet increasing compliance obligations.

The complexity of emerging threats continues to grow and threaten information assets globally, with an equally wide spectrum of motivations. A traditional reactionary approach to these threats carries significant risk through being unaware of malicious activity in your environment. Modern government and enterprises require a proactive approach to security situational awareness, to better protect their assets, personnel and customers.

The connected world has resulted in a rapidly evolving threat landscape

Challenges

The average cost of a successful cyber attack is now more than four million dollars and growing. Organisations face many challenges in addressing cyber security effectively, which is driving the growth of managed security and cloud security services globally. Many of these challenges are similar across organisations:

- Existing security solutions are disparate, not integrated, and provide no correlation or single view of events
- Difficulty developing good Governance models
- Meeting Compliance requirements
- Poor overall cyber hygiene
- Lack of skilled resource and expense of hiring
- Lack of visibility or situational awareness across mobile endpoints, infrastructure, network, perimeter and cloud based access/activity
- Too many existing security point solutions that are complex, high overhead and lack integration – so making sense of the noise is a challenge

Technology overview

Security Information and Event Management (SIEM) technology supports threat detection and security incident response through the real-time and historical collection, correlation and analysis of security events from a wide variety of event and contextual data sources.

SIEM technology supports threat detection and security incident response

It combines Security Information Management (SIM) and Security Event Management (SEM), providing real-time analysis of security alerts generated by network hardware, applications, endpoint devices (including mobile) and infrastructure appliances.

It also supports compliance reporting and incident investigation through analysis of historical data from these sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyse events across disparate sources. All of which can managed by a single dashboard for improved environment visibility, data context and event response.

Deployment options vary with traditional on premise solutions replaced in favour of cloud/service based and hybrid solutions. Enterprise level businesses remain the major consumers of these solutions, however the SMB market is catching up in the race of adoption. This is driven by the growth in the web, mobile, cloud and application based usage.

NEC's SIEM service

NEC provides an 'endpoint to cloud' monitoring service, utilising a best of breed industry SIEM solution. Service offerings are tiered and features include advanced real time and historical correlation, log management and retention, advanced analytics, and global threat intelligence - all managed, monitored and maintained centrally by NEC skilled Security Operation Centre (SOC) experts in our Global Security Intelligence Centre (GSIC) in Adelaide.

Service features and benefits

- Advanced historical and real time correlation, improving context and threat awareness
- Centralised single pane of glass - increasing visibility, control, performance and efficiency
- Enhanced protection of staff and customer data
- Flexible service and support offerings
- Improved governance and compliance position
- Leveraged skilled SOC analysts saving on FTE investment
- Log management and retention for complete auditability
- Reduced cost of ownership
- Reduced time to detect and respond to threats/breaches
- Reduction in damages/cost of breaches
- Regular service tuning to reduce false positives
- Service is available 24 x 7

Service and support packages

We offer three service and support package options and will work closely with you to assess your business and security needs to ensure we recommend the best solution fit for your organisation. Any combination of service and support packages are available.

Service package options

	Essential	Standard	Premium
Network coverage - visibility across perimeter devices & switching	✓	✓	✓
Real-time alerting	✓	✓	✓
Event and data correlation	✓	✓	✓
Infrastructure visibility including: event logs, server events (Exchange, mail, SQL servers, AD, DNS, back up servers, VOIP/SIP)		✓	✓
Triage (proactive)		✓	✓
Endpoint to cloud visibility			✓
End to end visibility of malicious traffic			✓
Log retention (retention period client specified)			✓
Ad hoc data analytics			✓
Threat hunting (proactive)			✓
Customised detection criteria			✓

Support package options

		Essential	Standard	Premium
Coverage	Days / Hours	Mon-Fri, 8am-5pm	24x7	24x7
	Public Holidays	No	No	Yes
Reporting	Frequency	Monthly	Quarterly	Monthly
	Content	Basic	Custom	Custom
Incident Response		✓	✓	✓
Configuration Review		✕	Annual	Monthly
Use Case Review		✕	Quarterly	Proactive
Policy Review		✕	Annual	Monthly
Daily Platform and System Performance Analysis		✕	✕	✓

Service consumption models

Value Added Reseller (VAR)

- Re-seller of security systems
- Top tier vendor partners
- Integrated into NECare, NEC's maintenance and support service

Security Integration Services (SIS)

- End-to-end security design, implementation and testing services
- Billed through milestones

Managed Security Services (MSS)

- Remote management of customer owned security equipment
- Defined service levels
- Device / user based monthly billing

Security as a Service (SECaaS)

- Refined security services based on defined technology platform
- NEC owned systems
- Elastic consumption model billed monthly

Security Consulting Services (SCS)

- Stategic customer consulting
- Security scanning and assessments
- Fixed or T&M billing

Security Training Services (Cyber range)

- Hands-on training services
- Partner with University
- Leverage infrastructure and use case scenarios

NEC's SIEM service consumption models

Why NEC?

Organisations are typically unable to cope with the complexity of cyber security threats and struggle to fill knowledge and skills gaps, or make the initial investments needed to provide suitable support and technology.

Adoption of cloud services amongst the majority of organisations is also causing visibility and control issues, which hold back adopting new, innovative technologies due to unknown risks.

NEC has proven capability in the security space, backed by a $4.38 million investment in the new GSIC facility located in Adelaide. The centre offers a wide range of security services delivered using a state of the art SOC environment by NEC security experts. The GSIC also connects with global NEC Security Operations Centres that include Japan, Singapore, Europe, and the Americas to offer true global coverage and sharing of threat intelligence.

Furthermore, our cyber security services can easily integrate into our broader suite of ICT solutions and managed services. Our expertise in designing, implementing, and supporting high-quality end-to-end solutions ensures the best possible security outcomes for our customers.

NEC's Security Operation Centre in Adelaide

For more information, visit au.nec.com, email contactus@nec.com.au or call 131 632

Corporate Headquarters (Japan)	**Australia**	**North America (USA)**	**Asia Pacific (AP)**	**Europe (EMEA)**
NEC Corporation	NEC Australia Pty Ltd	NEC Corporation of America	NEC Asia Pacific	NEC Enterprise Solutions
www.nec.com	au.nec.com	www.necam.com	sg.nec.com	www.nec-enterprise.com

NEC Australia Pty Ltd reserves the right to change product specifications, functions, or features, at any time, without notice. Please refer to your local NEC representatives for further details. Although all efforts have been made to ensure that the contents are correct, NEC shall not be liable for any direct, indirect, consequential or incidental damages resulting from the use of the equipment, manual or any related materials. The information contained herein is the property of NEC Australia Pty Ltd and shall not be reproduced without prior written approval from NEC Australia Pty Ltd.