NODE4

N4Threat Detect
Key Features

N4Threat Detect

SIEM, security alerting, vulnerability assessment & analysis service

Many businesses operate unaware of breaches and intrusions perpetrated inside their environment. It is only when the consequences of these breaches manifest, that subsequent investigation often reveals the extent to which these vulnerabilities have been exploited. Gaining information about threats and vulnerabilities inside and outside of your infrastructure, allows businesses to mitigate against the risks before they become today's data breaches and tomorrow's news item.

The inevitability of targeted hacking means that businesses need to be pro-active and manage security beyond just firewall rules and malware detection. Delivering comprehensive security management requires specific skills and techniques normally unavailable to most organisations.

The cost of implementing many SIEM type systems is prohibitive let alone the additional cost of managing and level of operation required to interpret these systems. Node4 offers N4Threat Detect as a fully managed security service providing effective intelligence and consultancy at an OPEX monthly rate.

N4Threat Detect includes detailed Network Intrusion Detection System (NIDS) which examines packet behavior and detects "bad actor" probing and reconnaissance. We also provide Host Intrusion Detection System (HIDS) which examines system behavior and tracks configuration status to expose and report on system compromise and modifications of registry and configuration settings. This allows for visibility of malware, rootkits and other rogue processes from user activity.

Vulnerability Management is cyclical and requires regular scrutiny, which is why we provide regular expert consultancy, as part of the service, to remediate any issues the reports highlights. Regular application penetration testing is offered as part of the service to assure the security measures in place and identify security vulnerabilities which automated processes are unable to identify.

Full monthly reporting is included to provide management intelligence of both internal and external threats, including top; alarms, attackers, attack strategies, destination ports, attacked hosts. This information can provide compliance for FISMA, HIPAA, ISO27001 and PCI 2.0 and 3.0 accreditation.

Key Benefits

✓	**Cost Effective** Benefit from industry security experts and technology by using an OPEX monthly rental solution to mitigate the risks.
✓	**Scalability** A solution which scales with your business, add systems and features as a fully managed service.
✓	**Speed** Fast to deploy with the ability to easily switch on features you need.
✓	**Resilience** Award winning technology combined with security expertise provides customers with confidence behind their security border.
✓	**Secure** N4Threat Detect services are connected to global intelligence centers which ensures threat intelligence is up-to-date for complete security.
✓	**24x7x365 Service** Our monitored and managed service provides the Node4 Security Operations Centre (SOC) team response to incidents 24*7 and offers customers regular reporting intelligence with monthly reports.

For more information on N4Threat Detect or other products and services we offer please call our Sales Team today on 0845 123 2222 or email us at info@node4.co.uk

N4Threat Detect

Key Features

Risk Mitigation

Visibility

Aggregated event data from disparate systems and devices provides a comprehensive overview which is graded and interpreted by our Security Service consultants for each customer.

Control

Providing security analytics to event data in real time for the early detection of targeted attacks and data breaches, and to collect, store, analyze and report on log data for incident response, forensics and regulatory compliance.

Expert Consultation

Regular monthly face-to-face Security Service advisories provide criticle analysis and guidance to the threats and vulnerabilities pertinent to your infrastructure.

Regulatory Compliance

Reportable

Reports on alarms, estate assets, system availability, trends and performance as well as comprehensive overviews of logon failures to a host of systems.

Compliance

Reports are available to support specific compliance requirements such as PCI DSS 3.1, HIPAA, FISMA, ISO 27001 and SOX

Asset Control

Track alarms on assets for security events and vulnerabilities maintaining a valid inventory.

Cost Effective

OPEX Monthly

No expensive capital outlay, simple fixed monthly rental cost.

Scalable

Add systems and assets to your service as you grow.

Low Investment

Select initial services and add features when required.

Experts on Hand

Compliment your team by utilising our expert Security consultants as part of your security strategy.

Systems Intelligence

OWASP

Utilising the OWASP framework to measure known threats and highlight weaknesses on applications and systems.

OSSIM

Providing access to the Open Source Security Information Management (OSSIM) community for security threat intelligence.

OTX

Links to Alien Vault Open Threat Exchange (OTX) community (37,000 participants in 140 countries), for up-to-date threat intelligence.

ISO 27001 Information Security

Our ISO 27001 Security Certification ensures we meet stringent control requirements to manage information securely.