SOC
SECURITY OPERATIONS CENTRE

Managed SIEM

Always watching what matters most

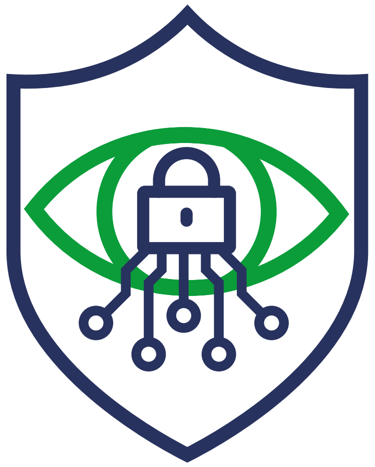
01 Nettitude Managed SIEM

Nettitude is an award-winning cybersecurity organisation with unparalleled capability in delivering managed security services. Through our global managed Security Operations Centres (SOCs) we deliver round the clock services that secure our clients and detect and respond to sophisticated cyber-threats, providing assurance that your organisation is protected.

Technology alone cannot mitigate the risk from cyber threats. Instead, businesses must respond through a well-managed security service considering all aspects of risk, using processes that extend through technology and into the workforce.

A managed Security Information and Event Management (SIEM) service provides a level of visibility and security that can be difficult to maintain in-house, both in terms of availability and expertise.

The Nettitude Managed SIEM service can be utilised for organisations that have limited resources and expertise to assist with the provision, management, monitoring, and integration of SIEM technology to provide world-class capability in detection and response.



02 What is SIEM and how does it work?

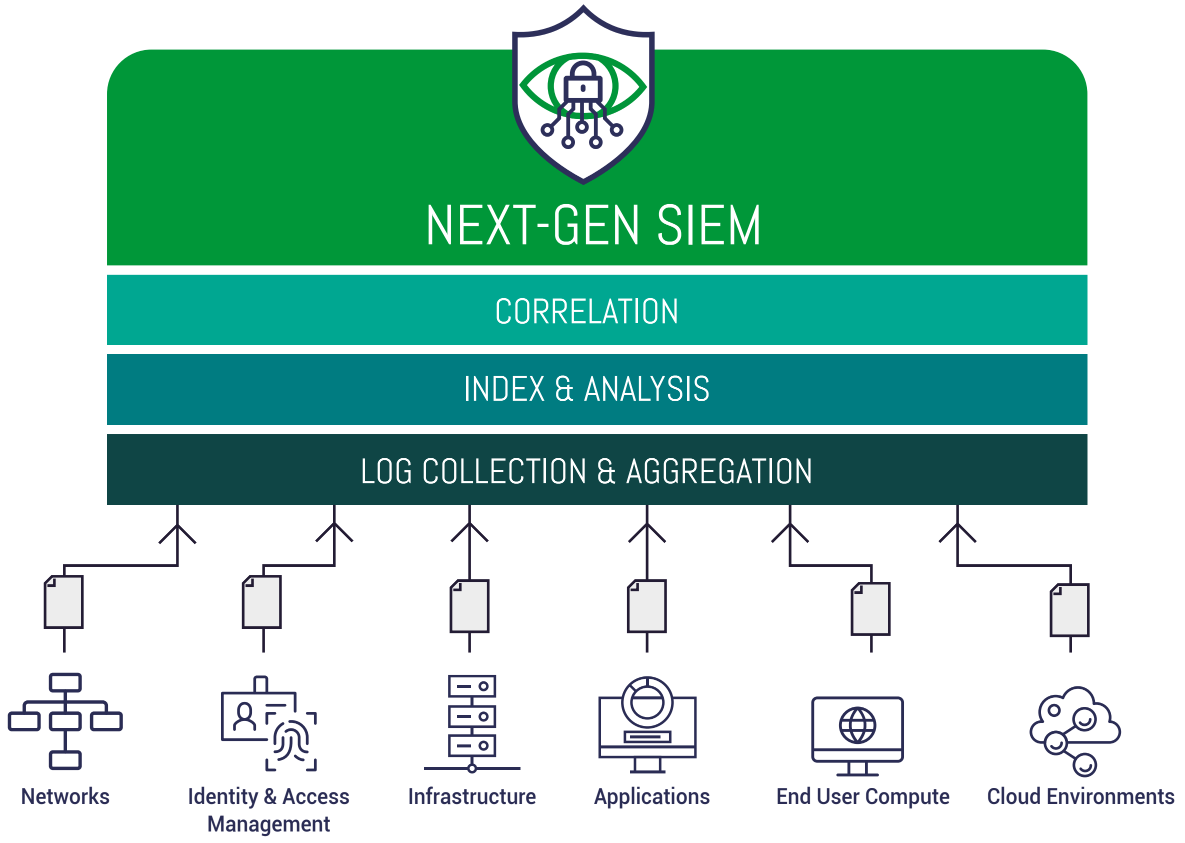
A SIEM provides an organisation with next-generation, unrivalled capability in detecting, analysing, and responding to security events and threats.

Next-generation SIEM systems combine Security Information Management (SIM) and Security Event Management (SEM) to provide real-time analysis capability of security alerts generated through collecting data, logs, and information from IT systems, applications, and network hardware.

SIEM software works by matching events against rules and analytics engines. It then indexes them to enable rapid search capability to detect, analyse, and respond to sophisticated threats and cyber-attacks using globally gathered intelligence.

This capability enables highly skilled security operations staff to track and record activity across an organisation's environment and IT systems through data analysis, event correlation, event and log aggregation and management.

These functions combined with reporting, automation, and orchestration provide a powerful security defence and monitoring capability required to protect against advanced threats.

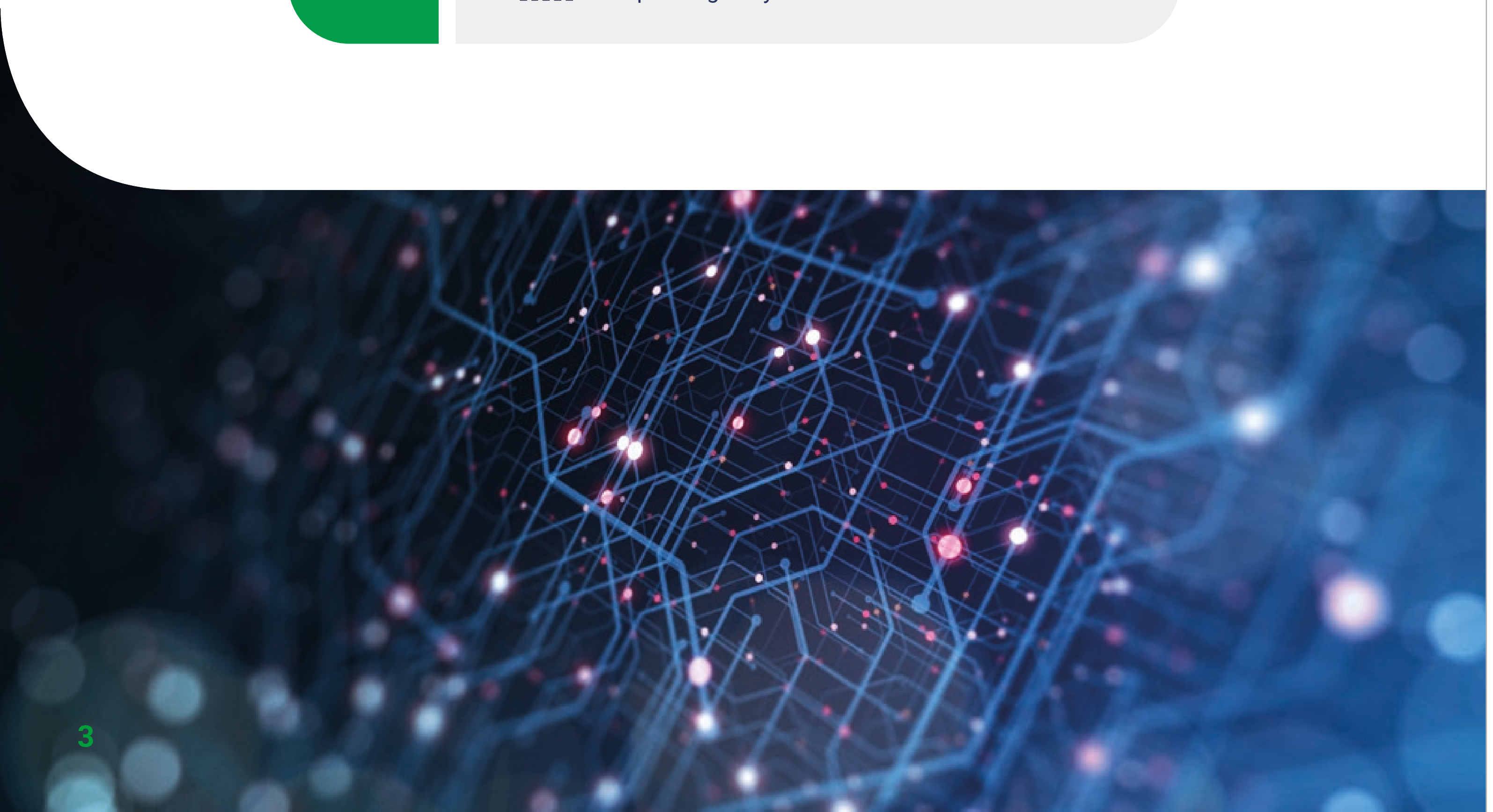


03 Benefits of a Next-Gen SIEM

In today's interconnected world, it is increasingly difficult for organisations to protect their data, as technology continues to rapidly evolve and change the working practices of organisations and people. This is where managed SIEM services come into play.

Next-Gen SIEM Benefits

- Real-time visibility and advanced detection across the Environment
- Centralised Management solution to collect logs and data from disparate systems
- Reduced mean time to detect (MTTD) and mean time to respond (MTTR)
- Collection and normalisation of data to enable accurate and reliable analysis
- Ease of access and ability to search across raw and parsed Data
- Ability to map security operations with existing security frameworks such as MITRE Attack
- Ensure compliance adherence with real-time visibility and pre-built compliance models
- Customised dashboards and sophisticated reporting ability
- Enhanced efficiencies in monitoring and responding to cyber events and threats



04 SIEM Technology and Features

Nettitude leverages next-generation SIEM technology provided by LogRhythm to deliver comprehensive logging, monitoring, and alerting capabilities. LogRhythm is an industry-leading and award-winning provider of security monitoring solutions.

We can provide SIEM PaaS (Platform-as-a-Service) where organisations do not have an existing SIEM solution. We can support your current LogRhythm on-premise deployments in a hybrid model working as an extension to your organisation's security team.

Nettitude is the current LogRhythm MSSP partner of the year and has won this accolade three times since 2016. Our most recent achievements have seen us win this award for two consecutive years due to our outstanding ability in integration, customisation, and application of the LogRhythm technology.

SOC
SECURITY OPERATIONS CENTRE
LogRhythm
MSSP of the Year 2020

LogRhythm is an enterprise-class solution that seamlessly combines SIEM, log management, file integrity monitoring, and machine analytics with host and network forensics in a unified Security Intelligence Platform.

It is designed to address an ever-changing landscape of threats and challenges with a full suite of high-performance tools for security, compliance, and operations.

LogRhythm delivers comprehensive, useful, and actionable insight into what is really going on in and around an enterprise IT environment including the below functionality:

- Advanced Intelligence engine
- Log Collection Technology to cover any environment or system
- Log Management
- File Integrity monitoring
- Case Management
- User & Entity Behaviour Analytics (UEBA)
- Endpoint Monitoring
- Smart Response & Automation
- Reporting and compliance for PCI DSS, HIPAA, GDPR, ISO27001 and other major compliance frameworks

05 Managed SIEM – Service Features

Nettitude's managed SIEM services provide the most highly accredited expertise combined with Gartner Magic Quadrant leading security technology to deliver industry-leading protection for your organisation.

Our approach is proactive, and threat led; informed by our offensive and threat intelligence teams to shape our defensive stance and protect against the latest industry threats, providing in-depth unrivalled detection and alerting capability where it is needed most.

24/7/365 Always on

24/7 x 365 Expert Security Analysis: always there, monitoring & alerting and advising for your peace of mind

Global Delivery

Nettitude has been at the forefront of cybersecurity SOC Operations since 2003. Our Managed SIEM services can be deployed and managed Globally through our global Security Operations Centres

Global Expertise

Certified expert knowledge within Offensive and Defensive Cyber operations, our SOC team are on hand as an extension of your teams to provide expert advice, guidance and remediation where required

Flexible Component Based

We can deploy PaaS SIEM software, and we can support your on-premise SIEM solutions ensuring these are integrated with existing security tools to provide best value for your organisation

Leading Technology

LogRhythm is a Gartner leader in SIEM technology providing comprehensive unified security intelligence platform that can monitor all of your IT environments and systems

Dashboard & Reporting

Custom real-time dashboards created in line with your business requirements combined with Nettitude Security & Service reporting to provide you complete visibility and insight to your security stance

Performance & Availability

Nettitude maintains best in class performance across SIEM availability, MTTD, MTTR and MTTE. Ensuring a rapid response to sophisticated cyber threats

Customisation & Engineering

Nettitude has certified experts that can assist in customisation, parsing and engineering to ensure complete coverage of bespoke systems and applications

06 Nettitude Value Proposition

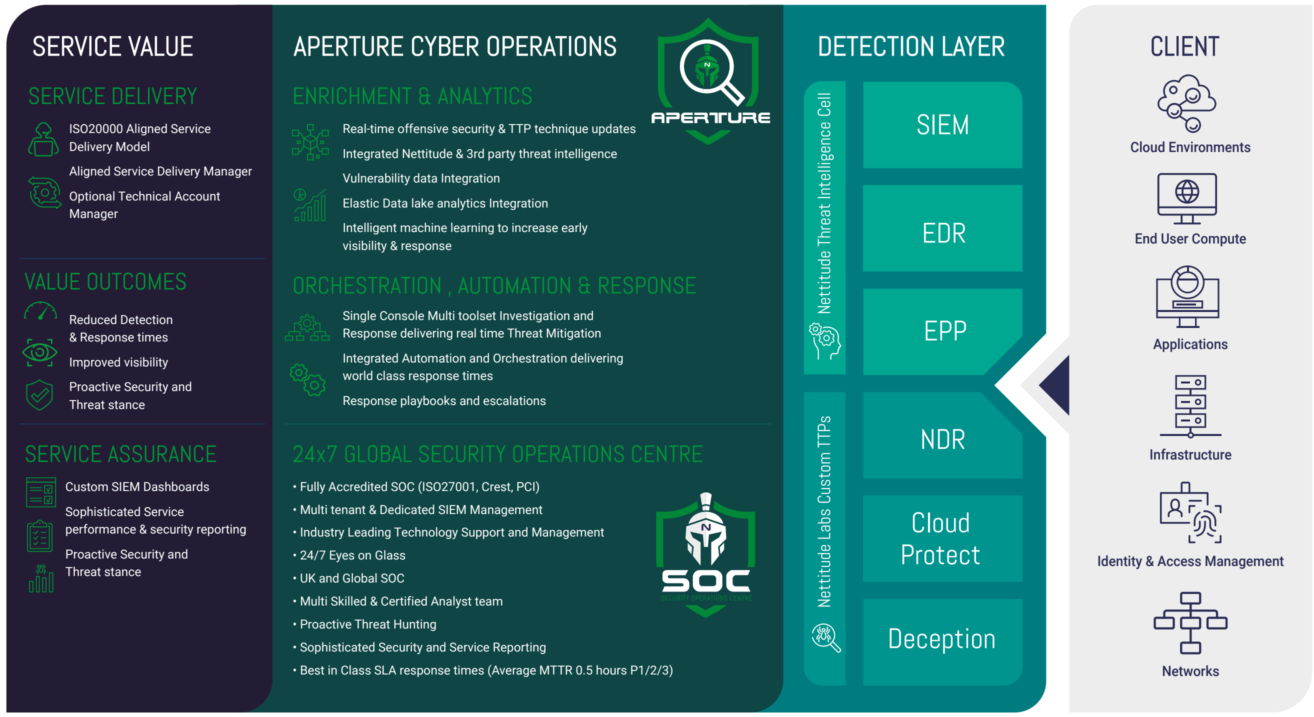
The Nettitude SOC provides advanced 24/7 monitoring and alerting to protect your business.

We use our custom developed Aperture Cyber Operations Management platform integrated with leading Gartner technologies to provide enhanced automation, orchestration & response capabilities to our SOC team.

The Aperture Cyber Operations platform provides enhanced enrichment, analytics, and intelligent learning to increase early visibility and response to cyber threats in an evolving world.

By combining these technologies with our highly accredited people and processes we can deliver best in class outcomes and value for your organisation.

APERTURE



SERVICE VALUE

SERVICE DELIVERY

ISO20000 Aligned Service Delivery Model

Aligned Service Delivery Manager

Optional Technical Account Manager

VALUE OUTCOMES

Reduced Detection & Response times

Improved visibility

Proactive Security and Threat stance

SERVICE ASSURANCE

Custom SIEM Dashboards

Sophisticated Service performance & security reporting

Proactive Security and Threat stance

APERTURE CYBER OPERATIONS

APERTURE

ENRICHMENT & ANALYTICS

Real-time offensive security & TTP technique updates

Integrated Nettitude & 3rd party threat intelligence

Vulnerability data Integration

Elastic Data lake analytics Integration

Intelligent machine learning to increase early visibility & response

ORCHESTRATION , AUTOMATION & RESPONSE

Single Console Multi toolset Investigation and Response delivering real time Threat Mitigation

Integrated Automation and Orchestration delivering world class response times

Response playbooks and escalations

24x7 GLOBAL SECURITY OPERATIONS CENTRE

- Fully Accredited SOC (ISO27001, Crest, PCI)
- Multi tenant & Dedicated SIEM Management
- Industry Leading Technology Support and Management
- 24/7 Eyes on Glass
- UK and Global SOC
- Multi Skilled & Certified Analyst team
- Proactive Threat Hunting
- Sophisticated Security and Service Reporting
- Best in Class SLA response times (Average MTTR 0.5 hours P1/2/3)

SOC
SECURITY OPERATIONS CENTRE

DETECTION LAYER

Nettitude Threat Intelligence Cell

Nettitude Labs Custom TTPs

SIEM

EDR

EPP

NDR

Cloud Protect

Deception

CLIENT

Cloud Environments

End User Compute

Applications

Infrastructure

Identity & Access Management

Networks

NETTITUDE
AN LRQA COMPANY

UK Head Office
Jephson Court,
Tancred Close,
Leamington Spa, CV31 3RZ

Americas
50 Broad Street,
Suite 403, New York,
NY 10004

Asia Pacific
18 Cross Street,
#02-101, Suite S2039,
Singapore 048423

Europe
Leof. Siggrou 348
Kallithea, Athens, 176 74
+30 210 300 4935

Follow us

solutions@nettitude.com
www.nettitude.com