SOC-as-a-Service

Detection and response for sophisticated threats

LRQA NETTITUDE SOC SECURITY OPERATIONS CENTRE

Contents

SOC-as-a-service

LRQA Nettitude is an award-winning cybersecurity organisation with unparalleled capability in delivering SOC-as-a-service. Through our global Security Operations Centre (SOC) we deliver round-the-clock services that secure our clients, and detect and respond to sophisticated cyber threats providing assurance that what matters most is protected.

SOC-as-a-service is a flexible component modular-based security service that is a managed extension of your organisation's internal team. It acts as a security partner that is dedicated to keeping your organisation and assets safe.

A SOC normally revolves around a Security and Incident Event Management System (SIEM) which only ingests log data from different endpoints and then alerts on suspicious activity. SOC-as-a-service provides enhanced and sophisticated managed detection and response services utilising multiple leading technologies to provide complete and holistic coverage of your security needs.

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. Organisations have typically responded by implementing security technology at strategic vantage points within the network infrastructure. Yet, despite this approach, companies are still being breached and data is being compromised.

A managed SOC services provides a level of visibility and security that can be difficult to maintain in-house, both in terms of availability and expertise. Organisations that have limited resources can procure managed SOC services for their alerting, detections, and incidents. Alternatively, you can supplement an existing team, providing in-depth expertise and availability when you need it most.

Evolving cyber threat landscape

The volume of cyber-attacks grows continually year-on-year. For organisations to maintain a strong security posture, they need to deliver round-the-clock security services. Attackers do not only act during core business hours, they attack organisations 24 hours a day, 365 days a year.

Security monitoring is a must in today's business world with threats, cyber-attacks, and data breaches becoming a regular part of the global news. But where do you start implementing security services to combat these threats?

Not all companies can afford to set up, hire security experts and operate a mature Security Operations Centre that can protect against the ever-evolving security threat landscape.

With our managed SOC-as-a-service you benefit from an award-winning SOC, which includes the crucial technologies and experts critical to protecting against these threats.

In Sophos' State of Ransomware Report 2021. Average ransomware recovery costs for businesses have more than doubled in the past year, rising from $761,106 in 2020 to $1.85 million in 2021.

The United States is a prime target for most hackers, as the country has experienced 227.3 million ransomware attack attempts. In other words, there are about 865 threats every minute in the first half of 2021. – 2021 Cyber threat report by Sonic Wall

Forty-eight per cent of UK organisations have been hit by ransomware in the last year, according to Sophos.

One small business in the UK is successfully hacked every 19 seconds, according to Hiscox. Around 65,000 attempts to hack small- to medium-sized businesses (SMBs) occur in the UK every day, around 4,500 of which are successful.

Data breaches cost UK enterprises an average of $3.88 million per breach, according to IBM and Ponemon's Cost of a Data Breach study.

Components

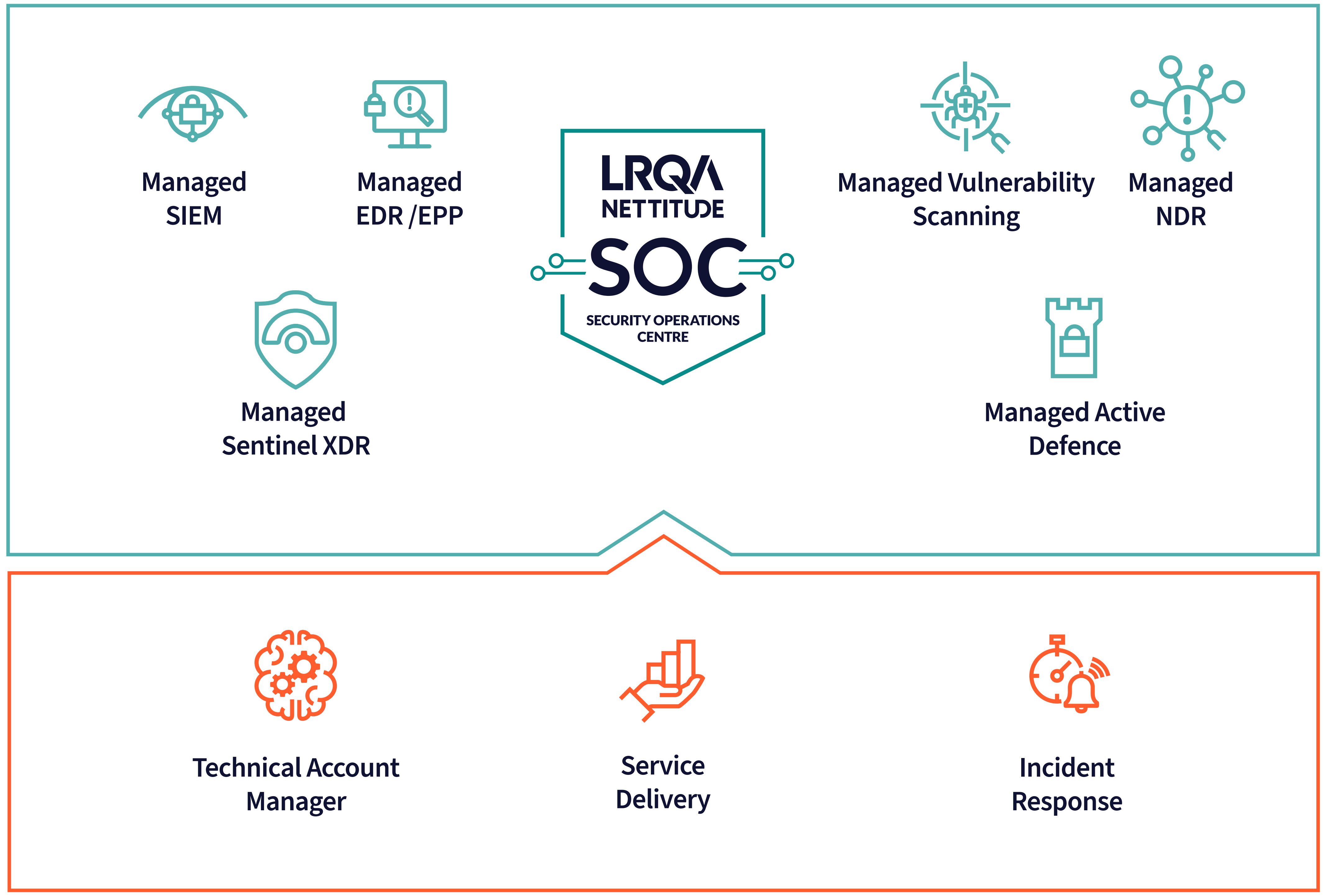
Whether you require a SIEM solution or a combination of tools and services to protect your entire organisation, LRQA Nettitude's SOC-as-a-service can be customised by selecting service components suitable to protect your environment and critical systems.

We utilise leading security technology vendors, combined with automation and orchestration to deliver a robust and comprehensive offering to suit your needs.

The flexible and component-based offerings can be selected or added to as your cybersecurity maturity evolves.

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.

We have extensive experience in delivering robust and adaptable security monitoring services, giving you the confidence required on what's important to you.



Features

LRQA Nettitude's SOC-as-a-service provides the most highly accredited expertise combined with Gartner Magic Quadrant leading security technology to deliver industry-leading protection for your organisation.

24/7/365 ALWAYS ON

Our SOC provides 24/7 x 365 expert security analysis; always there, monitoring & advising for your peace of mind.

GLOBAL DELIVERY

LRQA Nettitude has been at the forefront of cybersecurity SOC operations since 2003. Our SOC services can be deployed and managed globally.

GLOBAL EXPERTISE

Certified expert defensive SOC team on hand 24/7 as an extension of your teams to provide advice, guidance and remediation where required.

FLEXIBLE COMPONENT-BASED

Our component modular-based approach provides flexibility for your business requirements. We understand things can change over time and new features or components can be added at any time to enhance your cyber maturity.

TECHNOLOGY & THREAT INTELLIGENCE

Leading industry technologies and sophisticated threat intelligence is available to our SOC to ensure they always remain ahead of the latest cyber threats.

PERFORMANCE & REPORTING

Through the use of LRQA Nettitude's custom Aperture cybersecurity operations platform, we deliver industry-leading performance & reporting on alerting and response SLA's covering MTTR and MTTE across your service.

CERTIFICATION

Our SOC services are certified to ISO27001, ISO9001 and CREST SOC standards. We take our certification levels seriously and ensure we always maintain the highest certification for our SOC and the staff.

OPERATIONAL DELIVERY

Our services are proactively delivered to the structured process and governance models of ISO20k. All clients have an aligned SOC consultant and service delivery manager ensuring you get the support you need.

Aperture cybersecurity operations

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

We use our custom-developed Aperture cybersecurity operations management integrated with leading Gartner technologies to provide enhanced automation, orchestration, and response capabilities to our SOC team.

The 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.

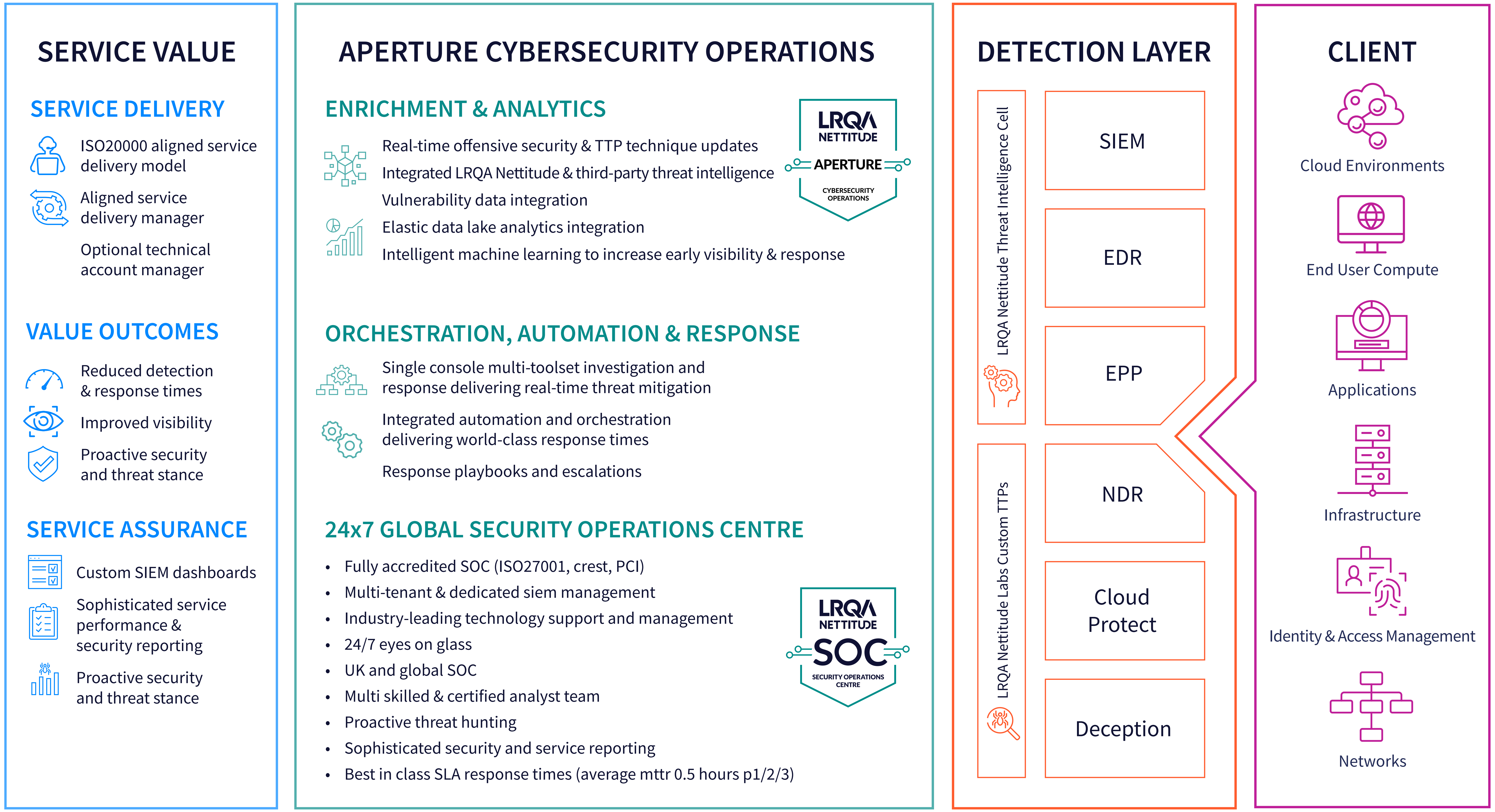
LRQA NETTITUDE APERTURE CYBERSECURITY OPERATIONS

LRQA Nettitude’s Security Operations Centre

Why use LRQA Nettitude’s SOC-as-a-service?

LRQA Nettitude prides itself on delivering value-add services for our clients. Many organisations can deploy and manage a reactive security monitoring technology, but to implement these technologies and then realise the returns on investment is difficult in an ever-evolving security landscape.

Our expertise and experience enable us to provide proactive, value-add services to our clients built on foundations across people, process, and technology.



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 CYBERSECURITY OPERATIONS

ENRICHMENT & ANALYTICS

- Real-time offensive security & TTP technique updates
- Integrated LRQA Nettitude & third-party threat intelligence
- Vulnerability data integration
- Elastic data lake analytics integration
- Intelligent machine learning to increase early visibility & response

LRQA NETTITUDE APERTURE CYBERSECURITY OPERATIONS

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)

LRQA NETTITUDE SOC SECURITY OPERATIONS CENTRE

DETECTION LAYER

LRQA Nettitude Threat Intelligence Cell

LRQA Nettitude Labs Custom TTPs

- SIEM
- EDR
- EPP
- NDR
- Cloud Protect
- Deception

CLIENT

- Cloud Environments
- End User Compute
- Applications
- Infrastructure
- Identity & Access Management
- Networks

People, process, and technology

PEOPLE

- Highly-certified
- L1-L3 analysts
- Security engineering
- Consulting
- Continual development
- Incident responders
- Incident managers
- Service delivery
- Technical account managers

PROCESS

- Threat modelling
- Playbooks and use cases
- Automation and orchestration
- Cyber incident response
- Service delivery
- Service and security reporting

TECHNOLOGY

- Aperture cybersecurity operations platform
- Next-gen SIEM
- Automation and orchestration
- Intelligent machine learning
- Endpoint detection and response
- Network detection and response
- Cloud compliance monitoring
- Active deception defence

People, process, and technology

PEOPLE

SOCs rely heavily on having capable people that are trained and experienced in identifying threats. It is essential that the people in a SOC have a deep technical experience that allows them to think like an attacker, and review network traffic to identify security events. In addition, when incidents are identified, it is necessary to have a robust incident management program to ensure artefacts are preserved and mitigation activity can be actioned.

LRQA Nettitude's deep understanding and experience of offensive attacks and ability to simulate sophisticated threat actors provides a firm knowledge base for our detection and response capabilities.

Our SOC invests heavily in its most valuable asset, our staff. They are highly certified and continually developed through learning and certifications to ensure we stay on the leading edge of cyber defence operations.

Our skilled teams include security and technical staff, incident responders, service delivery managers, and technical account managers to provide an all-encompassing tiered delivery model that remains flexible whilst providing best-in-class security services.

PROCESS

One of the most crucial aspects of a SOC is to have robust operating procedures and processes to govern and orchestrate the operational delivery and the detection and response lifecycles. In our experience, it is the quality of the process that ultimately influences the overall SOCs effectiveness.

THREAT MODELLING

It is essential that up front threat modelling and risk understanding is carried out in advance of setting up a SOC service. As part of this process, a thorough understanding of critical assets and attack surfaces are used to build out a strategic view of the organisation's estate and digital assets.

A SOC must embrace both proactive and reactive processes to deliver the optimum level of visibility across an organisation's estate. Reactive log review from strategic vantage points across an estate is critical to providing visibility across a monitored infrastructure. However, that alone will rarely suffice in today's current threat landscape.

LRQA Nettitude proactively completes hunt initiatives across critical assets and through network data captures. By blending proactive and reactive processes together, our SOC provides a holistic security approach to prevent critical asset compromise and data exposure.

USE CASES AND ORCHESTRATION

Understanding how attackers hide and move laterally across a network is critical in detecting advanced threats. Determining what normal user behaviour is, and then deviations away from this is a critical component of an effective SOC.

LRQA Nettitude has extensive experience in building use cases and processes that allow us to identify and contain attacks at multiple stages of the cyber kill chain.

Our orchestration and use cases are based around many common attacks patterns, and allow us to respond to malware breakouts, remote access toolkits (RATs), Command & Control (C2), lateral movement, privilege escalation, and attempted data exfiltration.

SERVICE OPERATION & DELIVERY

An Operational SOC performance can be hard to maintain without the right processes and procedures to ensure quality outcomes are delivered to the client. The majority of IT services utilised within a company are governed and provided using Industry aligned standards like ITIL and ISO20000k.

LRQA Nettitude has a mature ITIL/ ISO20000 aligned service operation and delivery framework that ensures we manage, maintain and deliver the best SOC services to our clients. We align and measure all our processes and performance in line with industry standards and we are continually investigating improvement opportunities.

People, process, and technology

TECHNOLOGY

Having the right type of technology that is fit for purpose and provides a rich data set to a security analyst is essential in detecting and responding to cyber threats.

In today's marketplace, there are many different technologies that a business could choose to utilise for their security protection, but with so many choices and such rich features to choose from how do you know which is the best for you?

VISIBILITY

LRQA Nettitude has invested in and tested best-of-breed cybersecurity technologies across the industry. We only use technologies we have heavily tested in real-world scenarios that we can be sure provide the best protection possible.

These technologies are combined with our custom-developed Aperture cybersecurity operations technology to ensure coverage and protection across all of the Gartner triad ensuring complete visibility of your environment.

LEADING VENDORS ALIGNED TO GARTNER TRIAD

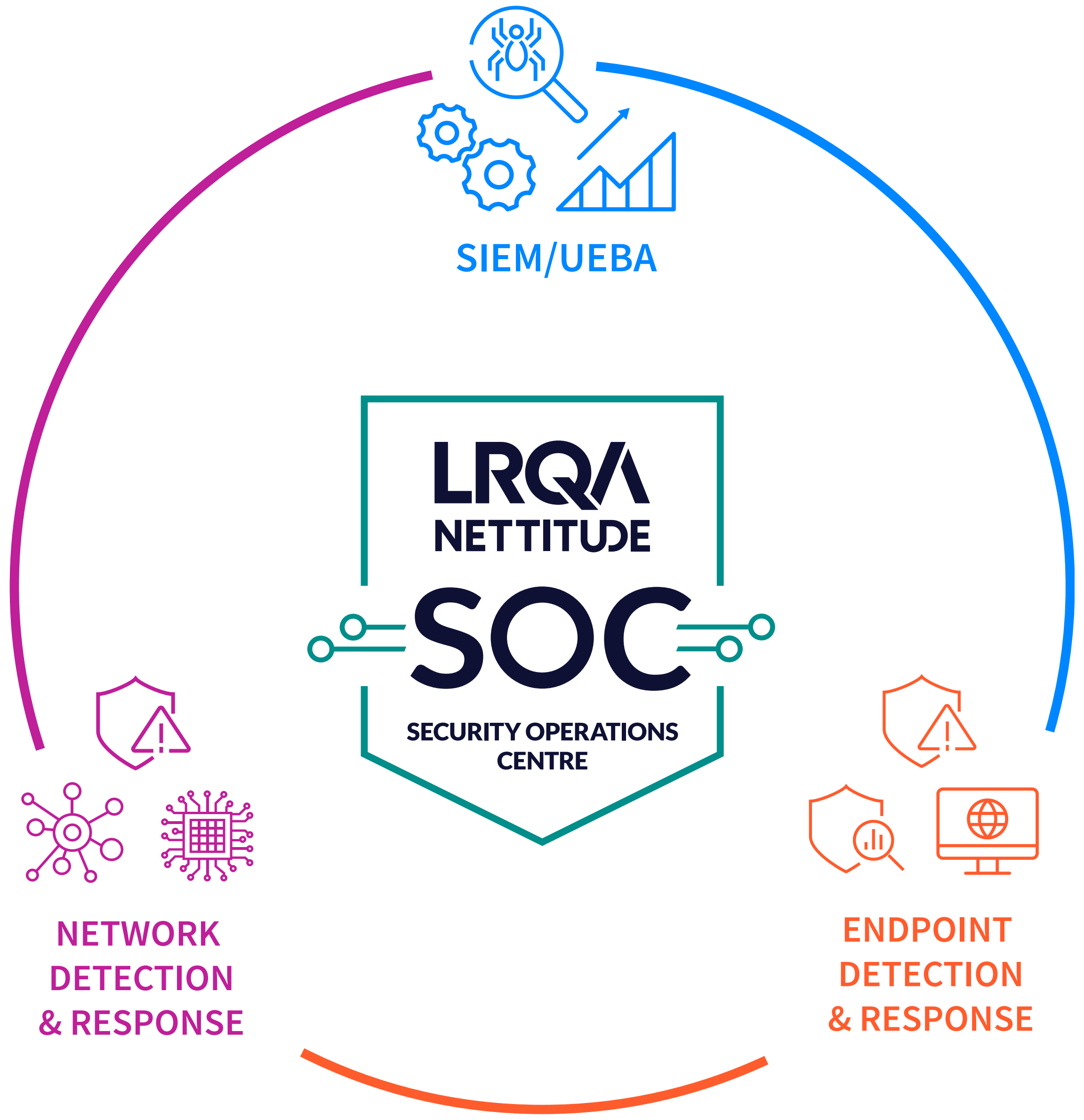
LogRhythm™

corelight

vmware® Carbon Black

CROWDSTRIKE

SentinelOne®


SIEM/UEBA
LRQA NETTITUDE
SOC
SECURITY OPERATIONS CENTRE
NETWORK DETECTION & RESPONSE
ENDPOINT DETECTION & RESPONSE

Technology capability

MANAGED SIEM

- Next-gen SIEM powered by LogRhythm
- Feature rich next-gen capability to provide comprehensive logging, monitoring and alerting.
- Gartner magic quadrant leader
- As a service or on-premise deployment models
- Aperture cybersecurity operations integration
- Secure data & log retention for three years

MANAGED SENTINEL XDR

- Collect data at cloud-scale across all users, devices, applications, and infrastructure
- Investigate threats with artificial intelligence and hunt for suspicious activities at scale
- Respond to incidents rapidly with built-in security orchestration and automation of common tasks
- Customisable data storage options providing cost-effective hot, warm, and cold storage

MANAGED EDR & EPP

- Feature-rich next-gen capability to provide comprehensive ability to detect, protect, investigate and stop sophisticated cyber attacks in their tracks
- Gartner magic quadrant leader
- Cloud-based or local deployment models
- Detect and isolate threats across all endpoints
- Forensic analysis, behavioural and indicator-based
- Extensively tuned to client requirements

MANAGED ACTIVE DEFENCE

- Leading cyber threat deception technology to defend against sophisticated cyber attacks
- Configurable and managed misdirection & confusion tactics to help slow or stop a cyber attack
- Gain advanced and early visibility into cyber attacks
- Extensively tuned to client requirements
- Management and control of all deployed deception assets deployed across networks, infrastructure and active directory

MANAGED NETWORK DETECTION & RESPONSE

- Powered by Corelight or LogRhythm Mistnet technology
- Capture real-time network traffic across your estate to gain greater visibility into threats
- Real-time actionable intelligence & full packet capture network monitoring
- Flexible deployment models
- Powerful dashboard investigation visualisations and reporting capabilities

MANAGED VULNERABILITY SCANNING

- Vulnerability scanning powered by Tenable One
- Feature-rich next-gen capability provides comprehensive ability to actively identify, investigate and prioritise vulnerabilities
- Unified visibility of your attack service
- Cloud-based rapid deployment
- Powerful dashboard visualisations and reporting capabilities
- Agents and scanner-based deployment models

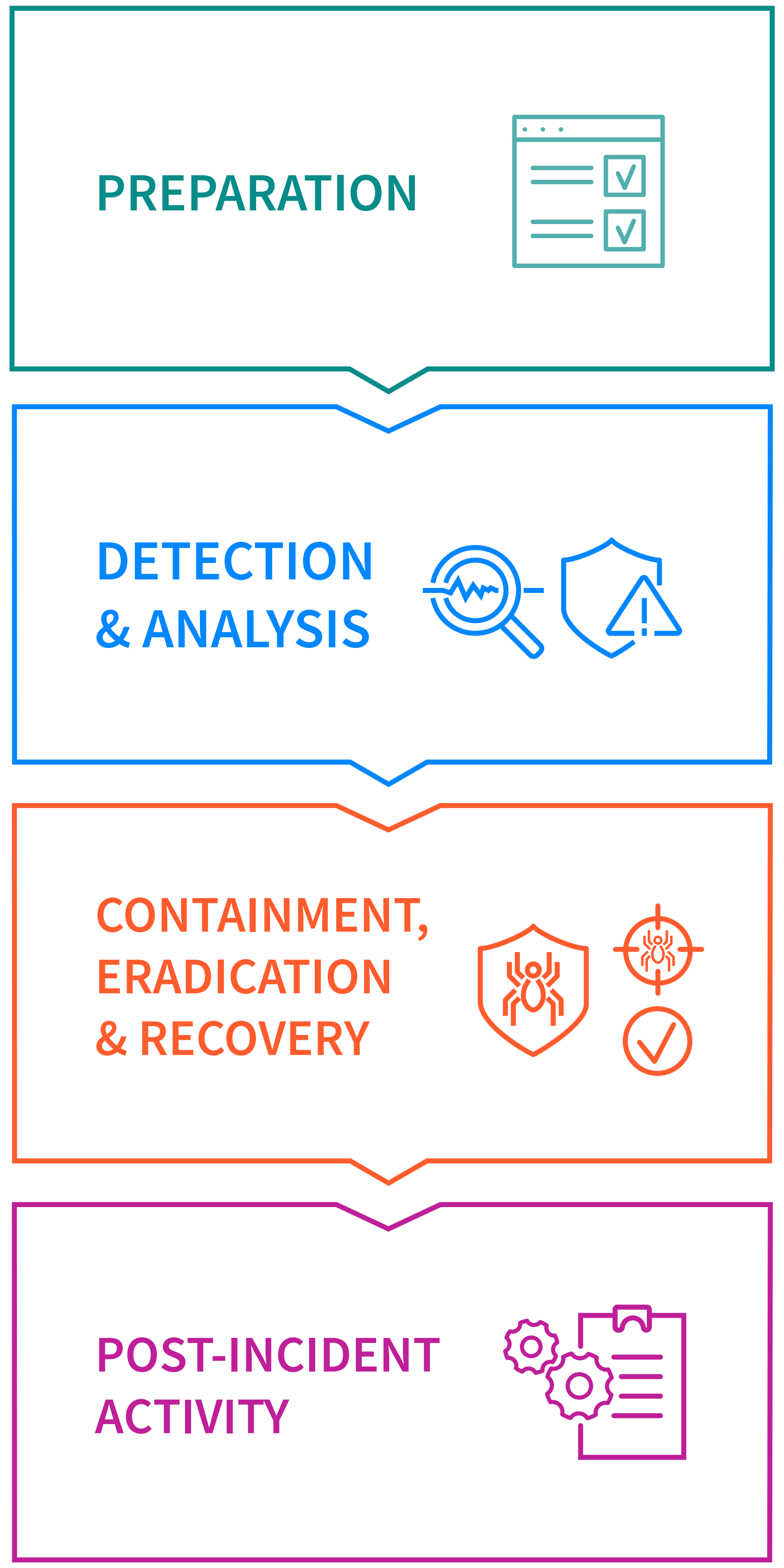
Cyber incident response

The LRQA Nettitude SOC provides a world-class Incident Response (IR) service powered by the LRQA Nettitude Cyber Incident Response Team (NCIRT) team, tailored to suit the needs and threats your organisation could be facing.

The NCIRT team are certified and experienced in all aspects of cyber incidents and we follow and adhere to best practice industry guidance and standards from NIST, FIRST, SANS, NCSC, and CREST.

Using leading industry technology and certified experts, the NCIRT manages, contains, remediates, and reports on cyber incidents providing assurance when it is needed most.

- Certified expert team on hand 24/7 as part of your team to support your business response to a cyber attack
- Expert advice and guidance covering technical remediation, incident management, risk & business continuity planning during an event
- Dramatically reduce the time, and therefore the costs, of resolving incidents maintain productivity whilst specialist staff resolve incidents
- Expeditious containment of the incidents will prevent the spread, and thus cost, of a cyber incident
- Early resolution of incidents prevents further losses of data from a compromised system
- Your organisation could qualify for a lower cyber insurance premium by having aligned experts in place
- Conform to industry best practice and emerging legal requirements



LRQA NETTITUDE
NCIRT
CYBER INCIDENT RESPONSE TEAM

CYBER RESPONSE ENGAGEMENT MANAGER

CYBER RESPONSE INCIDENT MANAGER

- Certified incident response analysts & consultants
- Cyber response engagement manager
- Cyber response incident manager
- 24/7 response SLA
- Cyber risk assessment & guidance
- Assisted onboarding & preparation
- Incident response business continuity preparation
- Host, network, malware analysis & reverse engineering

Incident response service features

We provide a full range of tactical and strategic solutions tailored to your business needs and network environment, ensuring a robust security posture when you need it, enabling you to get back to normal operations quickly, with confidence.

GLOBAL EXPERTISE

LRQA Nettitude has been at the forefront of cybersecurity since 2003. Our NCIRT team has the know-how and expertise to quickly identify, investigate and remediate the breach.

RAPID RESPONSE

Our NCIRT team understand that a rapid response is critical to containing and limiting the impact of a cyber incident. Our experts can start work within hours backed by guaranteed response SLAs and rapidly analyse for signs of compromise or breach.

HANDS-ON REMEDIATION

NCIRT can provide guided and assisted hands-on technical remediation support to help guide your teams to implement recommendations to contain and eradicate then reduce the risk of future compromise.

COMMAND & CONTROL

We assign you dedicated cyber incident and engagement managers with years of industry expertise in managing crisis situations to aid in the command, control & communications over all cyber incident response activity.

TECHNOLOGY & THREAT INTELLIGENCE

Leading industry technologies and sophisticated threat intelligence is available to our SOC to ensure they always remain ahead of the latest cyber threats.

REPORTING

Cyber response and incident level reporting covering impact, recovery, technical analysis & investigation and executive-level summary encompassing all facets of a cyber incident management.

RESEARCH & REVERSE ENGINEERING

We can provide host, network and malware analysis and reverse engineering through our dedicated Research & Innovation centre.

SERVICE FLEXIBILITY

Our services provide flexibility for you and any unused IR hours can be used on alternative IR professional services to ensure you maximise value from your service.

CREST
VA
PEN TEST
STAR Intelligence-led PT
STAR Threat intelligence
CSIR
SOC
OVS

PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council
APPROVED SCANNING VENDOR

CYBER ESSENTIALS

ISO 9001 ISOQAR REGISTERED
ISO 27001 ISOQAR REGISTERED
Cert No. 23208

ISO 14001:2004 REGISTERED FIRM

Get in touch

Visit **www.nettitude.com** for more information
or email enquiries to **solutions@nettitude.com**

UK Head Office
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES

Americas
810 Seventh Avenue
Suite 1110
New York
NY 10019

Asia Pacific
460 Alexandra Road
#15-01
mTower
Singapore 119963

Europe
Fidiou 9
Athina
106 78
Greece

LRQA NETTITUDE