SOC
SECURITY OPERATIONS CENTRE

Managed Active Defence

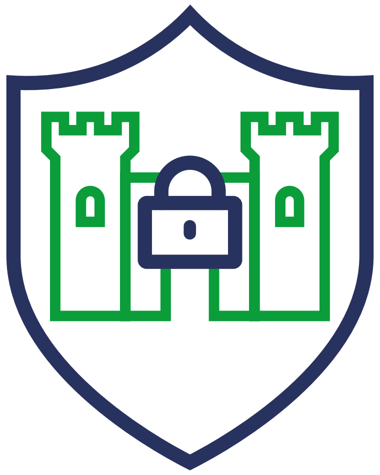
Proactive defence to combat advanced threats

01 Managed Active Defence

Nettitude is an award-winning cybersecurity organisation with unparalleled capability in delivering managed security services. Through our global 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.

A Managed Security Service can provide an organisation with a level of visibility & security that can be difficult to maintain in-house, both in terms of availability and expertise. Organisations that have limited resources and knowledge can procure Managed Security Services to manage their security technologies, providing in-depth expertise and availability when you need it most. Many organisations do not have large security teams or the security expertise in house with skills across all areas required to design, build, improve and enhance their security technologies, security risks and their defensive posture against the continually evolving threat landscape.

The Nettitude Managed Active Defence service deploys a next-generation deception platform provided by Attivo Networks to provide an active defence to your security services.



02 What is Managed Active Defence?

A shift from the defensive to an offensive security posture is necessary if organisations with sensitive and high-value data assets are to gain the upper hand in their battle against modern security threats. In assuming such a stance, organisations now look to deception and decoy systems for post-infection breach detection.

Nettitude Managed Active Defence is a next-generation solution using the Attitvo Networks platform. It provides advanced detection, protection, and SOAR use cases across a wide variety of network environments. The service is delivered 24/7 365, providing deception plans and orchestration playbooks all year round, tailored to your needs.

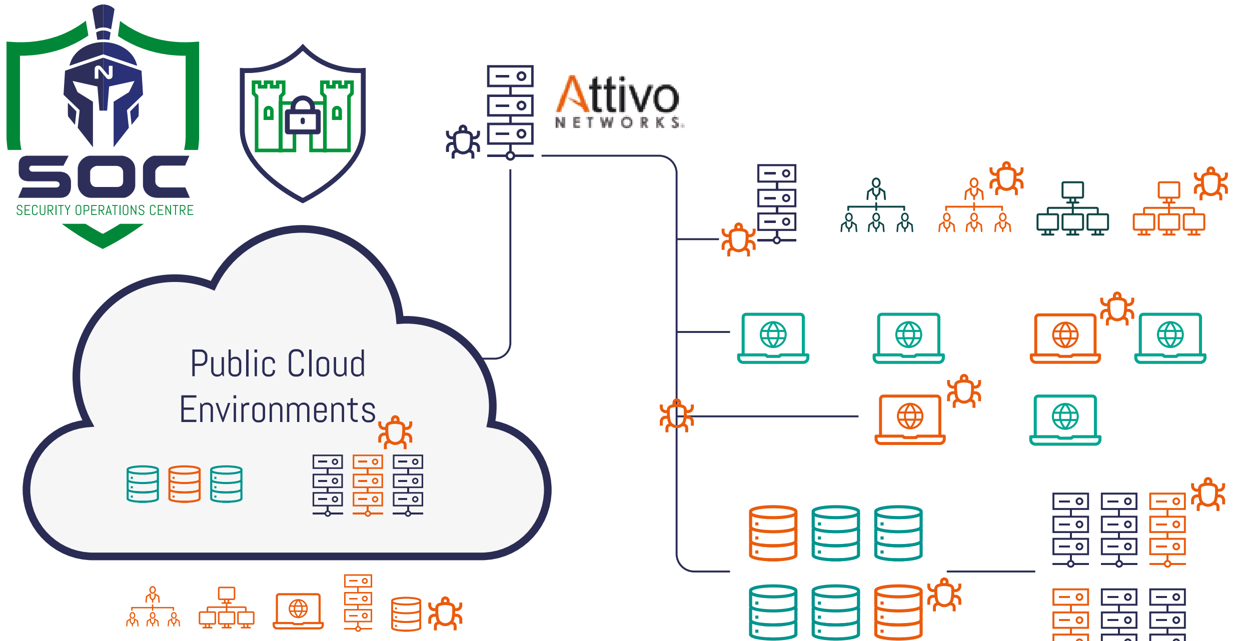
Deception platforms, such as our managed Attivo deception platform, are designed to detect and analyse all attack activity. This includes reconnaissance, lateral movement, stolen credential usage, malware and ransomware attacks, and man-in-the-middle activity.

The Attivo Networks ThreatDefend® platform uses fully customisable virtual machines to mimic production assets. This ranges from Windows and Linux servers to IoT and SCADA devices and projects them throughout the network. The solution enables security organisations to lay tripwires throughout the network turning the entire IT environment into a trap. Deception allows you to turn the tables on attackers and force them to be 100% correct in their movements or risk detection by the security team.

> *"Judicious use of networks, pocket litter, and honeytokens can waste the adversary's time and resources, expose their pedigree, and create false knowledge on their part. Deception can also add randomness and unpredictability to an architecture, network traffic, service, or mission activity, making an adversary's understanding of the environment more challenging and at best inaccurate"*
>
> Mitre, The Cyberspace advantage: Inviting them in

03 About Attivo Networks

Attivo Networks® provides an innovative defence for protection against identity compromise, privilege escalation, and lateral movement attacks. The company's solutions deliver unprecedented visibility, prevention, and derailment for security exposures, attack paths, and attack escalation activities across endpoints, Active Directory, and cloud environments.



Decoy Assets and deception techniques deployed environment wide covering active directory, cached credentials, network architecture and systems

04 Why do you need Managed Active Defence?

Attivo is a next-generation detection and prevention solution. It utilises deception techniques to fool an adversary into thinking they have control and access to the legitimate system and network resources.

The attacker is fed false information around Active Directory, cached credentials, connections to other systems, network architecture, and important assets and is led to interacting with fake hosts documents.

The attacker is therefore held in a state where they are unable to conduct malicious activities against live assets, giving the defending teams more time to deal with the threat.

Using the ThreatOps integrated connectors, our clients can deploy automated orchestration playbooks, enabling quick response actions to attacks, reducing MTTR and protecting critical data and assets.

Gain time for Responders

Preventing the attacker from identifying that they have been discovered

Reduce the risk of harm

The attackers are not interacting with production assets, preventing catastrophic data loss, encryption or destruction events

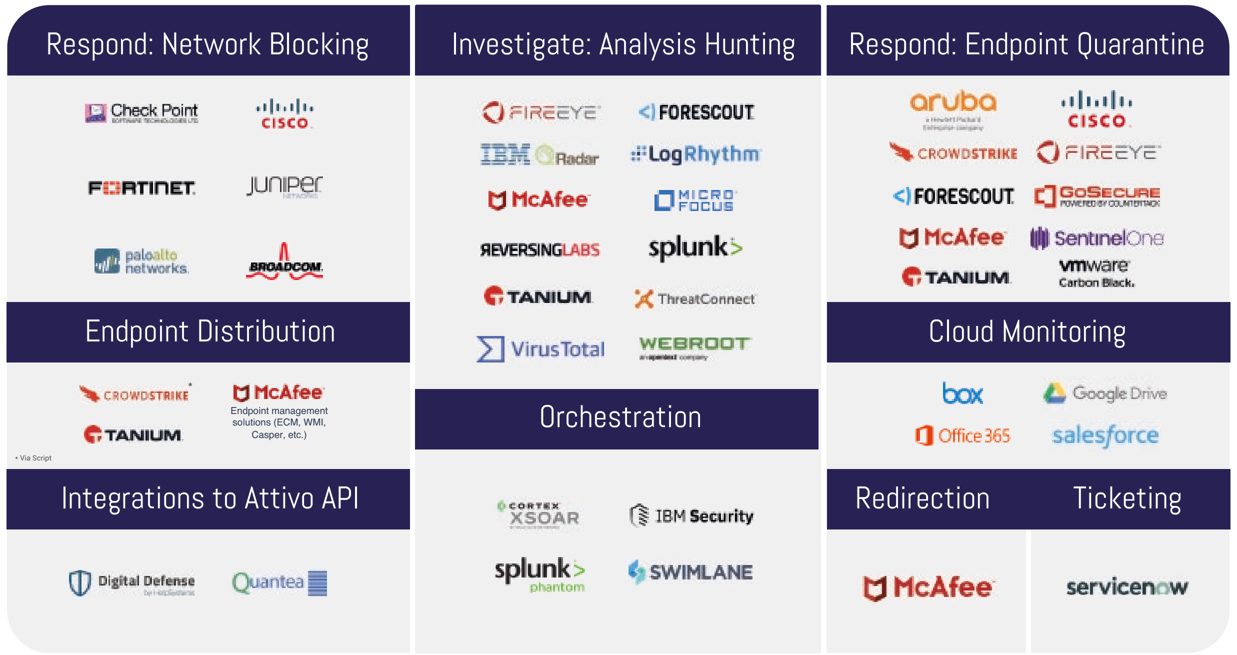
Gather Intelligence

Monitor the adversary to gather vital intelligence around their TTPS

Automate response actions

Integrating Attivo into existing security tools using ThreatOps enables quick response to an attack

Integrations and Playbooks for Automated Incident Response


Respond: Network Blocking

Investigate: Analysis Hunting

Respond: Endpoint Quarantine

Endpoint Distribution

Orchestration

Cloud Monitoring

Integrations to Attivo API

Redirection

Ticketing

Endpoint management solutions (ECM, WMI, Casper, etc.)

* Via Script

05 Benefits of Managed Active Defence

Rapid Detection and Attack Deflection – the deceptive assets should not normally have any interaction, therefore when an attacker touches them the solution will generate rapid high-fidelity alarms

Managing the adversary – directing the adversary via authentic breadcrumbs deployed to endpoints towards deceptive assets prevents them from impacting critical resources and therefore isolating their activities, enabling an effective response

Learn adversary techniques – deception can cause an adversary to expose their pedigree, create false knowledge and capture their TTPs

Insider threats – provides rapid detection and risk reduction for insider threats

Advanced detection – provides detection in areas not well served by other products

Automation & Integration – allows for the implementation of automated response and mitigation activities within a client environment

Managed Active Defence

'Active defence to combat advanced threats'

The Active Defence service significantly reduces the likelihood of an adversary completing their attack, leading to a data breach or other malicious action, as well as reducing the time to detect and respond to an incident. These metrics (known as Mean Time to Detect or MTTD and Mean Time to Respond or MTTR) are key indicators of an effective detect and respond capability.

The specific objectives of the service will be customised to each client collated through the BI workshops and service reviews on an ongoing basis. This is because every client faces different threats and operates a unique set of critical assets. Nettitude understands this and therefore can customise the detection through a unique set of use cases.

Business Challenge - Managed Active Defence Solution

Business Challenge	Solution	Value Prop/Benefit	Industry Stats
Active Directory Protection	• Detect malicious AD queries • Conceal real AD objects • Return misinformation to derail attacks • Capture attacker signatures and intent	• Detect and Prevention • Risk mitigation • Attack surface reduction • Constant visibility into security exposures in AD • Quick ROI & remediation of security exposures in AD	81% of hacking-related breaches used stolen or weak passwords (DBIR 2020)
Insider Threats	• Alters the apparent threat surface so insider cannot tell what is real vs.fake, causing them to make mistakes and reveal their unauthorized activity	• Attack surface reduction • Detection and prevention	30% of data breaches involved internal actors (DBIR 2020)
Lateral Movement	• Detect Credential Exposures • Deny Credential Stealing, AD Data harvesting/ privilege escalation • Deploy decoys and apply concealment policies to restrict data access • Derail Internal Discovery	• Attack surface reduction • Visibility of identity-related attacks	60% of attacks now involve lateral movement (CarbonBlack Global Threat Report 2019)
Ransomware	• Hides and denies access to local files, folders, removable devices, and mapped network or cloud shares. • Creates fake network file shares that feed the ransomware limitless data	• Stall the attack for prompt isolation of infected systems • Mitigate extensive and costly damage	Ransomware is the second most common malware incident variety
Remote Worksite Compromise	• Detect and derail cyber-attackers targeting VPNs • Protect SaaS and cloud credentials	• Attack surface reduction • Remote worker protection	Over 53% of remote employees unaware of security policies for mobile device management - IBM Security 2020 survey

06 Managed Active Defence – Service Features

Nettitude's Managed Active Defence service provides 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. It protects against the latest industry threats to provide an in-depth defence with 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 SOC services can be deployed and managed Globally through our Global Security Operations Centres

Management

Provision, monitoring, maintenance and management of Infrastructure, Attivo Central Manager and BOTsink deception deployment

24/7/365 Technical Support

Fully managed technical and vendor support raised through the Nettitude SOC

Proactive Defence

Not just the alerting, but proactive activities run continually within your managed service offering - actionable event review daily, weekly event & endpoint review, network, decoy and endpoint campaign reviews monthly/quarterly

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

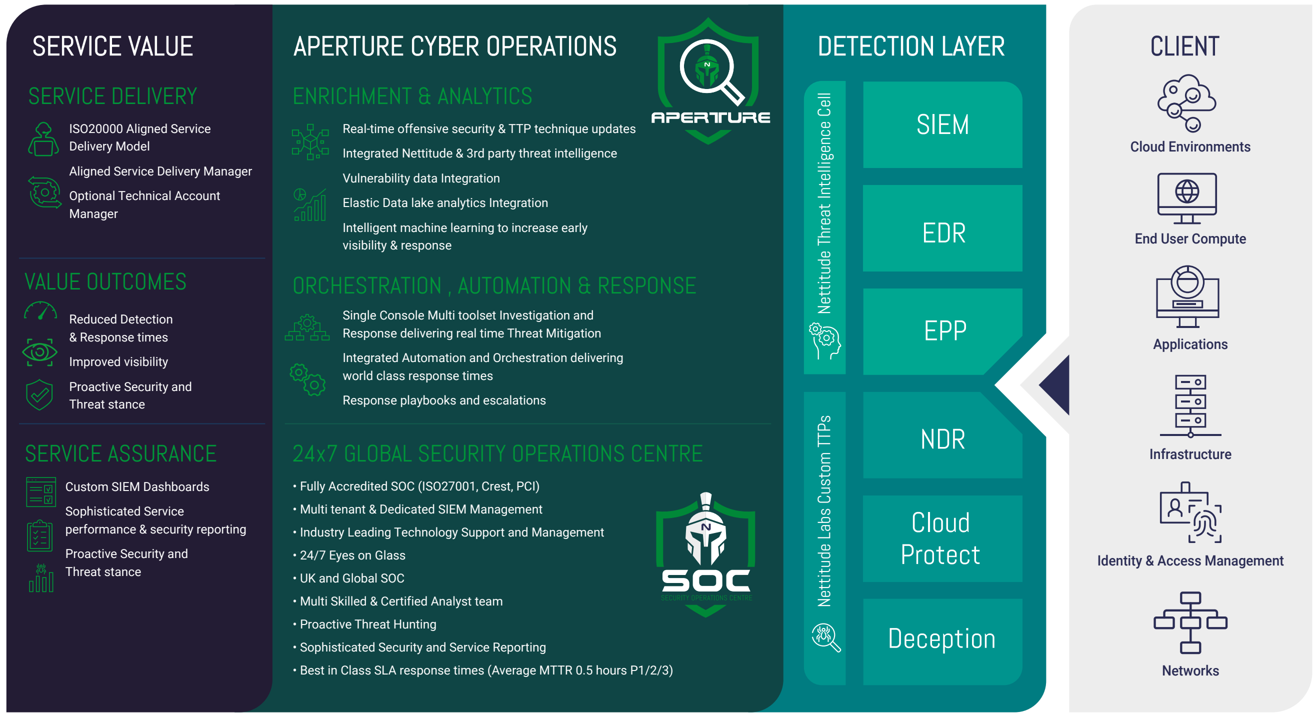
07 Nettitude Value Proposition

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.



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

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)

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

08 Nettitude Managed Service Activities

Actionable Event review – Performed 24/7 by Nettitude SOC team

Analysts daily (or often, multiple times a day as alerts are generated) review the events generated and recorded in the Attivo Central Manager system that are severity medium or higher. These events often contain information of an actionable nature and are the first line indication of malicious activity present on a company's network.

Medium and higher severity events can indicate a severe network, server, or application misconfiguration which is causing multiple computing resources to communicate in an unhealthy or counter-productive manner (such as repeated ARP flooding and system scanning.)

In addition, these events are often directly related to policy violations, compromised computing systems, malicious software activity, or other security-related events. These events are meant to indicate activity that violates one or more policies on a network and should be investigated and mitigated appropriately.

Weekly Event Review - Performed Weekly by the Nettitude SOC team

Often performed weekly, analysts review the low and very low events recorded for the previous week to evaluate if any unexplained anomalies from a medium or higher event had any additional lower priority impact associated with that activity.

These events are often evaluated during the 24/7 actionable event review. However, lower-level events may appear before or after an actionable event and by performing a weekly review, may highlight other issues that can be investigated and mitigated. Note: low and very low events are not generally used for actionable event indicators as they are common on most networks. But they do provide context when higher priority events are identified. They may point to an in-depth context on an attack, misconfiguration, or a malicious event.

System Health Check performed Daily by Nettitude SOC team

A daily system health check is performed for all Attivo systems, each product has a system status indicator to highlight when any warnings (yellow status) or critical errors (red status) are present on the Attivo system.

Clicking on the status indicator will provide analysts and system administrators with detailed information related to the status, which can be acknowledged, researched, or a support ticket opened to help resolve the issue.

Weekly Endpoint Review - Performed Weekly by the Nettitude SOC team

Performed weekly, analysts review and check the endpoint reporting console to identify if any endpoints have been disconnected from the Attivo BOTsink or ACM.

They review Last Seen Date, comparing dates and times to the update interval defined for the Client Group Configuration setting. For example, if a client group has an update interval of 60 minutes, the Last Seen Date timestamp should be within the past 60 minutes. If any endpoints are found to be disconnected or not updated, that endpoint can be investigated to see if it is still online and able to communicate with the Attivo platform.

Where issues are discovered, these will be raised and managed by the Nettitude SOC team to the client's technical teams to remediate.

Network, Decoy and Endpoint campaign review - Performed Monthly/Quarterly by client & Nettitude SOC Team - Recommended Quarterly by Vendor

Every quarter, Nettitude and the client will perform a network segment & endpoint campaign review. This review aims to ensure that any network changes are captured and configured within Threat Direct forwarder. Also, endpoint campaign reviews are completed to ensure that decoy VM customisations are still relevant and to capture any changes, this could be new server VLANS on new network segments etc. Any new requirements or new decoy deployments would then be scoped by the Nettitude SOC on behalf of the client.

NETTITUDE
AN LRQA COMPANY

CREST. VA PEN TEST STAR STAR CSIR SOC

Security Standards Council QUALIFIED SECURITY ASSESSOR

Security Standards Council APPROVED SCANNING VENDOR

winner Cyber Security Awards

Computing Security Awards FINALIST

CYBERSECURITY BREAKTHROUGH AWARD 2020 THREAT INTELLIGENCE COMPANY OF THE YEAR

ISO/IEC 27001 Information Security Management

ISO 9001:2008 REGISTERED FIRM

ISO 14001:2004 REGISTERED FIRM

INVESTORS IN PEOPLE

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
1 Fusionopolis Place,
#09-01, Singapore,
138522

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

Follow Us

solutions@nettitude.com
www.nettitude.com