

Sentinel XDR – Accelerator Deployment

Guided rapid deployment of Sentinel by Nettitude cyber experts



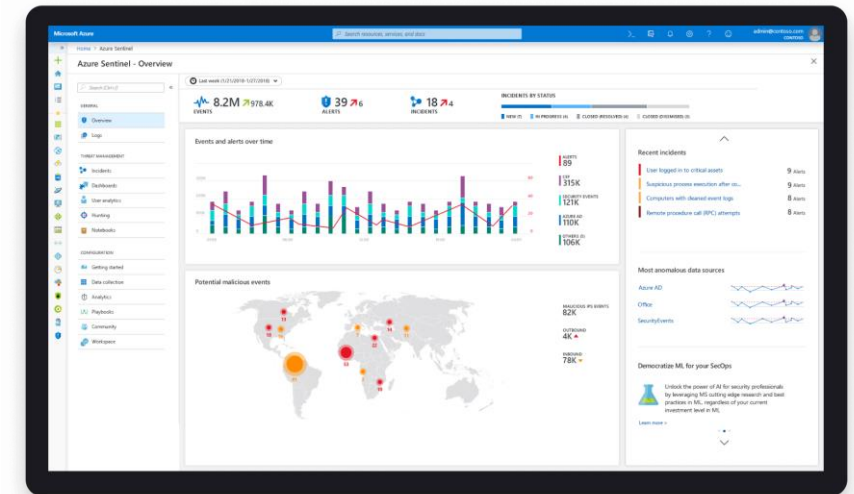
You will:

- ✓ Get quickly up and running to minimise onboarding time and maximise your investment in Microsoft Security technologies.
- ✓ Have the pain removed from Sentinel's complex planning, design, and deployment.
- ✓ Gain the benefit of expert resources to take the load off your security teams with a fully planned and proven delivery methodology delivered by highly certified CREST and Microsoft Security experts.
- ✓ Gain the benefit and access to the Nettitude mature tried and tested standard detections suite.



What's included:

- ✓ 10 days of Sentinel cyber consultancy delivered by a Nettitude Security Operations Centre (SOC) consultant.
- ✓ A structured 5-phase deployment of Microsoft Sentinel including a threat-led business intelligence workshop, Sentinel deployment & integration, onboarding of log sources, detection deployment, and a handover workshop.
- ✓ Onboarding and integration of Azure core data connectors and up to five additional client-selected log sources.
- ✓ Deployment of the Nettitude standard detections and alert rules providing instant detection capability.



Sentinel XDR – Accelerator Deployment

Guided rapid deployment of Sentinel by Nettitude cyber experts



Initiation

Project Kick Off

- Project kick-off call
- Project and technical scoping
- Resource alignment

Phase 1

Business Intelligence

- Business Intelligence Workshop (BIW)
- Threat consultation
- Critical asset mapping
- Log collection planning
- Use case and detection planning
- Business intelligence workshop report



Phase 2

Deployment and Integration

- Azure Sentinel High-Level Design (HLD)
- HLD documentation creation
- Sentinel, Log Analytics deployment and configuration
- Access control configuration
- Integration of STIX/TAXI TI feeds



Phase 3

Onboarding

- Integration & connection to Azure core data connectors
- Deployment of remote log collectors
- Onboarding of log sources
- Optimisation of log sources



Phase 4

Detection Deployment

- BIW use case mapping
- Alert & detection deployment of Nettitude standard detections
- Initial tuning of Sentinel alert rules
- Alert and detection testing
- SOAR automation creation



Phase 5

Project Closure & Handover

- Project handover call
- Documentation handover
- Knowledge transfer

← Average Deployment Timeline 2-4 Weeks →

Sentinel XDR – Accelerator Deployment

Why Nettitude?



Experience:

- Nettitude is an **award-winning** provider of cybersecurity services, bringing innovative thought leadership to the ever-evolving cybersecurity marketplace.
- In-house **dedicated cybersecurity innovation & research team** with specialists enabling us to stay at the forefront of cybersecurity.
- Operating SOC and security services for more than **20 years**.
- **Deep understanding and experience** of offensive attacks and the ability to simulate sophisticated threat actors provide a firm knowledge base for detection and response capabilities.

Certification & Accreditation:

- A **Microsoft Solutions Partner Security**.
- **Highest levels** of industry certifications across Microsoft and Azure security tools.
- **SC 100/200/200, AZ 103/104/305/500, MS500**.
- The **only organisation in the world** to hold a **full suite of CREST** accreditations.
- **First SOC provider worldwide** to be accredited by CREST for the SOC discipline.

