SERVICE BRIEF

Microsoft Sentinel.

Turnkey cloud-native SIEM and SOAR connectors, analytics, automation and SOC handover.

THE PROBLEM & THE APPROACH

Security telemetry scattered across Microsoft, cloud and third-party systems is hard to correlate. Without a unified SIEM, threats are detected late and responses stay manual.

CNNECT's Microsoft Sentinel Implementation is a turnkey engagement that configures, builds, tests and hands over a production Sentinel environment. Data connectors, analytics rules, automation playbooks and Defender XDR integration delivered in two to three weeks with a documented SOC operating model.

Key challenges addressed

EIGHT COMMON RISKS

01 Security telemetry scattered across Microsoft, cloud and third-party tools.

02 Late threat detection from manual log review and untuned correlation.

03 Inconsistent or absent automated response to common incident patterns.

04 Defender XDR and Sentinel deployed separately, not unified in operations.

05 Threat intelligence feeds not integrated into detection logic.

06 Behavioural analytics (UEBA) disabled or unused across data sources.

07 No baseline workbook for SOC, executive or cost reporting.

08 SOC operating model ad-hoc; no runbook, RBAC or handover documentation.

SERVICE OVERVIEW

Detect. Investigate. Respond.

Microsoft Sentinel is the cloud-native SIEM and SOAR platform, managed alongside Defender XDR in the Microsoft Defender portal. CNNECT installs the right solutions from Content Hub, connects the data sources that matter, deploys and tunes analytics, and builds the automation that closes incidents faster.

Delivered in two to three weeks remotely. You receive a production Sentinel workspace with data connectors, analytics rules, automation playbooks and an As-Configured pack ready for your SOC team.

PHASE 01 · DISCOVERY

Discovery.

Identify in-scope data sources (Microsoft 365, Azure, third-party, on-premises), priority use cases, and the automation playbooks that should be built and attached to analytics rules.

- Data source & connector mapping
- Priority use case selection
- Automation playbook design
- Scope sign-off & runbook

PHASE 02 · BUILD AND TRANSITION

Build & transition.

Enable Sentinel, install Content Hub solutions, configure connectors, analytics, playbooks, workbooks and UEBA. Validate through pilot and hand over with documentation, RBAC and SOC enablement materials.

- Sentinel + Defender unified
- Analytics, TI & UEBA tuned
- Logic Apps playbooks live
- As-Configured pack & SOC handover

TYPICAL TIMELINE

2 – 3 weeks

From kick-off to SOC handover.

INVESTMENT

From £10,000

Final price agreed after scoping.

WHAT'S INCLUDED

FIVE DELIVERABLES

01 Discovery report

02 Sentinel workspace

03 Connectors & analytics

04 Automation playbooks

05 As-Configured pack

NEXT STEPS

Discuss your SOC needs or request a sample Sentinel build plan.

hello@cnnect.com

+44 20 7173 5320

CNNECT.COM