

# Microsoft Sentinel Proof-of-Concept

Make SecOps more efficient with industry's first cloud-native SIEM+SOAR (security information and event management + security orchestration and automated response) solution. Bring together alert detection, threat visibility, proactive hunting, and threat response in a single solution. *Microsoft Sentinel is 48% less expensive and is 67% faster to deploy compared to traditional SIEMs.*<sup>1</sup>



## Limitless scale

Collects data at cloud scale – across your entire hybrid and multi-cloud infrastructure.



## Focuses on real threats

Cuts through billions of low-fidelity signals to create actionable, high-fidelity incidents – *Enables a 79% reduction in false positives.*<sup>1</sup>



## Automates response

Built-in automation of common tasks and workflows and triaging of incidents.

## Rapidly close the cyber defense gap with Netrix and Microsoft Sentinel

Netrix was the co-development partner for Microsoft Sentinel and our security experts are sought after industry leaders. In this proof-of-concept, we will help you understand the capabilities of the solution, and determine the best-suited approach to optimize your security operations with Sentinel.

### What's covered

 **Duration: 2 Weeks**  **Cost: \$15,000**



#### Understand & plan

- Analysis of requirements and priorities of key stakeholders for Sentinel deployment.
- Plan for the proof-of-concept, which would include key use cases, syslog sources covered, and Windows/Linux servers covered.



#### Build

- Build of the foundational Sentinel components.
- Configuration of MMA on provided Linux machine on-premises and enable forwarding to Microsoft Sentinel.
- Configuration for data ingestion, including support for up to 10 Data Connectors.
- Configuration of up to 5 Analytics/Alerts



#### Deploy

- Onboarding of the necessary sources into Sentinel.
- Configuration of up to 5 syslog sources, reporting into Microsoft Sentinel.
- Set-up of up to 3 automation runbooks.



#### Share

- Discovery of threats and demonstration of automated response using Sentinel.
- Design documentation with as-built and configuration information.

**Netrix can take your Microsoft-powered infrastructure to the next level, providing you the engineering and services expertise to help you customize, automate, and analyze your entire environment.**



Get in touch with us:

info@netrixglobal.com | netrixglobal.com