How to use this template

Customize this template by adding your assets to the following sections:

- **HEADER** | Add company name, product name, and logo
- **INTEGRATION or OFFERING** | Insert header and summary paragraph to address how your product helps address industry challenges
- **CUSTOMER BENEFITS** | Add bullet points
- **LEARN MORE** | Include your CTA
- **COVER** | Remember to remove this slide from your final document.

MISA APPROVAL

- Before publishing, email the completed slide back to MISA for final approval.

Microsoft Azure Sentinel

Cloud-native SIEM with built-in AI so security analysts can focus on what matters most.

Azure Sentinel is a cloud-native security information and event manager (SIEM) platform that uses built-in AI to help analyze large volumes of data across an enterprise—fast. Azure Sentinel aggregates security data from all sources, including users, applications, servers, and devices running on-premise or in any cloud, letting you reason over millions of records in a few seconds. It includes built-in connectors for easy onboarding of popular security solutions and supports standard formats like CEF and Syslog.

Collect data at cloud scale—across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence from Microsoft.

Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.

Respond to incidents rapidly with built-in orchestration and automation of common tasks.

Onevinn MDR powered by Microsoft Security Solutions such as Microsoft Azure Sentinel to help provide intelligent and proactive protection.

Onevinn's Managed Detection and Response (MDR) utilizing Azure Sentinel is a managed service helping companies to shift from a reactive state of cyber security into a proactive state of security and protection. Onevinn MDR Built on Azure Sentinel is helping enable protection against modern cyber security threats and attacks by providing the customer with insight and control of their security and threat landscape.

Onevinn MDR is built on Azure Sentinel and is operated 24/7x365 by a dedicated team of experienced cyber security analysts. The service contains adapted detection and response playbooks for accelerated containment against modern attacks and threats. To help the customer maintain a proactive security posture the delivery of the MDR service is built around three integrational fundamentals: governance, advisory and continual service improvement.
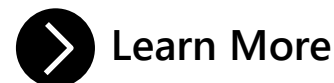
CUSTOMER BENEFITS

- 24/7x365 Managed Detection and Response as a Service

- Cyberattack kill chain visibility

- Automated remediation processes

- Proactive delivery methodology

- Onevinn's developed and adapted IP's for enhanced protection

- Managed Service utilizing Azure Sentinel and Microsoft 365 Defender

Learn More

For more information

https://www.onevinn.com

Contact

Olov Norman
olov.norman@onevinn.se
Christopher Lindström
christopher.lindstrom@onevinn.se

Member of
Microsoft Intelligent
Security Association

Microsoft