VENZO_

Azure Sentinel Kickstart Kit

Get started utilizing Azure Sentinel as your cloud-based SIEM

"The main barriers to reach SOC excellence are: lack of skilled staff (57.7%) followed by absence of effective orchestration and automation (49.6%)."

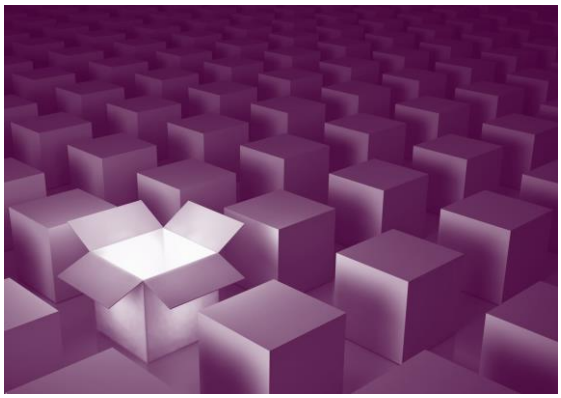
- SANS Institute SOC Survey 2019

With the rise of new targeted threats and complex attacker techniques, even the most advanced security tools cannot detect all malicious software and behavior in your organization. Therefore, it is essential to implement **tailored** detection and threat hunting use cases as well as **relevant** alerts that help your security team react quickly and efficiently.

Security incident responders often drown in the high number of alerts. They mainly work on alert triage and incident identification, which leaves not much time for actual containment of threats and application of the correct response actions. It is crucial to implement **effective orchestration and automation** to assist these pressured teams.

This is where a modern SIEM system can help **improve your security posture** with automated alert grouping, correlation of large amounts of data and automated incident response workflows that help to remove routine tasks.

What you will get



This kit will help you start using Azure Sentinel as your new cloud-based SIEM. It contains:

- **3-hour workshop on Sentinel** (select from 3 topics)
- Initial **setup of free data sources** and analysis of all available data for creation of relevant use cases
- Development and implementation of **5 use cases**
- **Actionable recommendations** for your SIEM implementation roadmap

---

Experienced security analysts show you how to best utilize your new SIEM

Learn how threat hunting queries and automation can increase proactivity

Gain visibility into undetected activities by correlating data from multiple sources

Improve your security posture with new detection and response mechanisms

Get advice for your SIEM implementation scope, requirements and priorities

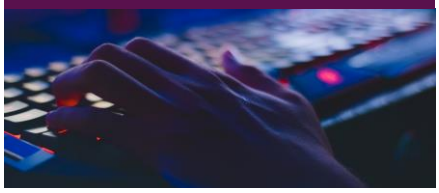
Azure Sentinel Kickstart Kit Details

Workshop Topics

The kickoff meeting will be used to select a topic for your tailored workshop. The workshop will introduce you to best practices in the chosen area and show you how you can utilize Sentinel.

Sentinel Configuration and Log Ingestion

Security Incident Handling in Sentinel



Threat Hunting in Sentinel

Available Data Sources and Log Ingestion

Depending on which Microsoft products you already use, data from one ore more of the below products can be ingested into Sentinel SIEM as part of the Azure Sentinel Kickstart Kit:

- Microsoft Cloud App Security
- Microsoft 365 Office Activity
- Azure (Security Center)
- Azure Defender for Identity (previously Azure ATP)
- Microsoft Defender for Endpoints (previously Microsoft Defender ATP)
- Azure Active Directory (fee issued by Microsoft for Azure AD data ingestion and usage)

Use Case Examples

VENZO's security analysts work daily with security incident detection and response. Based on their experience, they will create five relevant security use cases in your Sentinel SIEM—utilizing the available data that has been ingested. Some examples for such use cases are:

- Suspicious logon to Outlook mailbox using PowerShell or WinRM (Office 365 data required)
- RDP port opened and public IP address assigned to virtual machine (Azure data required)
- External user added to a confidential or sensitive Teams group (Teams data required)
- Attempt to sign-in to a disabled account from an uncommon IP address (Azure AD data required)
- Enumeration of Azure storage key from anomalous IP (Azure data required)
- Mails from multiple mailboxes forwarded to external mail account (Office 365 data required)

Contact us today to get started

VENZO_ | Hejrevej 34D, 2400 Copenhagen NV | cybersecurity@venzo.com