KiZAN

Gold Microsoft Partner

Microsoft

Azure Sentinel Enhanced Accelerator

Accelerate the design and deployment of Azure Sentinel and modernize your security operations, enhanced with on-prem networking signals.

Azure Sentinel is a cloud native security information and event management (SIEM) and security orchestration automated response solution (SOAR) solution, reinvented for a modern world. Put the cloud and large-scale intelligence from decades of Microsoft security experience to work. Make your threat detection and response smarter and faster with artificial intelligence (AI).

The benefits of deploying Azure Sentinel are:

- **Improved visibility** - Collect data and gain insights at cloud scale across all users, devices, applications, and infrastructure.
- **Boost threat protection** - Detect previously uncovered threats using analytics and unparalleled threat intelligence from Microsoft.
- **Proactively investigate threats** - Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.
- **Accelerate your response** - Respond to incidents rapidly with built-in orchestration and automation of common tasks.

Azure Sentinel Accelerator Deliverables:

- Complete Sentinel overview and planning session.
- Sentinel deployed to Log Analytics workspace.
- Microsoft data connectors added to Azure Sentinel.
- Analytics and fusion rules for data connectors enabled.
- Up to 4 Sentinel playbooks created.
- Review of workbook insights, alerts, and queries outlined in activities.
- Review of Solarigate post-breach hunting queries results.
- Configuration documentation and next steps.

KiZAN will assist your organization with implementing and optimizing Azure Sentinel. From planning to deployment, through customization and education, KiZAN can help ensure you have a solid base deployment to demonstrate what sentinel has to offer.

Contact Us

KiZAN Technologies
www.kizan.com