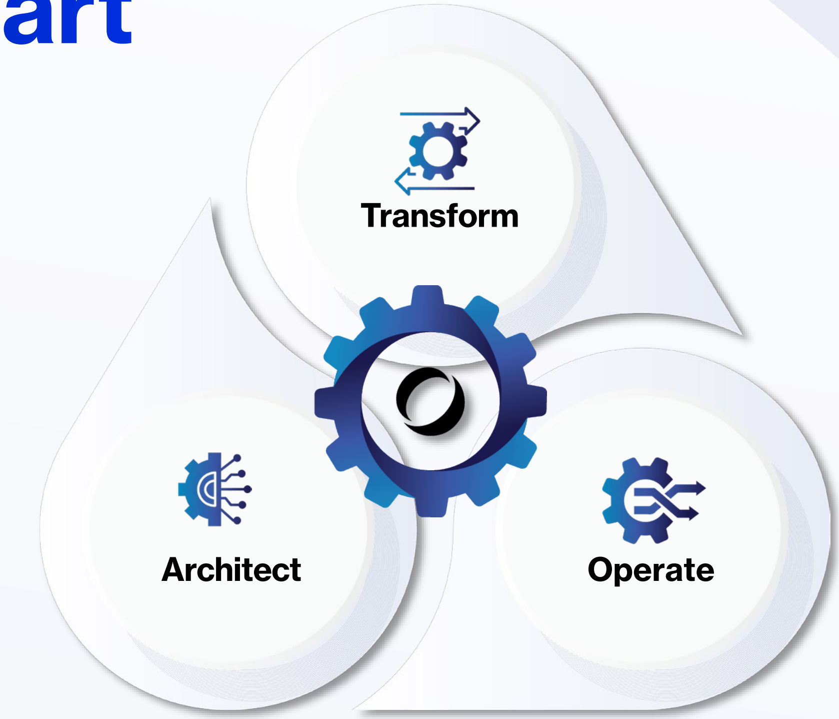
Microsoft

ivision

# Sentinel Cloud SIEM QuickStart

## Our Approach

ivision's QuickStart security offering for **Microsoft Sentinel** enhances cybersecurity readiness through incident response, centralized security visibility with scalable integrations, advanced threat detection, and automation runbooks for agile responsiveness to attacks. Our solution bolsters your existing security posture, will safeguard critical assets, and maintain stakeholder confidence in the ability to protect against the day-to-day dynamic threat landscape.



## Common Challenges

- Lack of a comprehensive security information event management platform and proven framework for response
- Lack of cohesive collection of event data, and significant alert fatigue from multiple stand-alone security tools
- Lack of AI and Analytics capabilities to detect the anomalous and threats in real-time while avoid chasing all the noise
- Significant Improvements needed to threat response in real-time with focused intelligence and robust investigative tools built-for-scale.
- Operationalizing XDR (Extended Defense and Response) into a modern SOC

## Benefits

- ✓ Enhanced and Integrated Security tools and protection policies for assets and platforms built in the Microsoft Cloud
- ✓ Improved ROI, maximizing your MSFT investment with integrated XDR
- ✓ Increase business productivity by reducing downtime and impact critical platforms and systems essential for operations and revenue generation.
- ✓ Cost-effective options for retention of event management resources, and powerful AI capabilities to greatly expand defense against future threats.

## Detect / Protect / Respond

## What's Included

- Alignment with regulatory compliance requirements to support security operations
- Development Security Event Management and Incident Response Strategy
- Implementation for MSFT Sentinel for SIEM and event data source integration
- Tactical and Prioritized baseline policies and SIEM configurations to reduce alert fatigue and centralize event and alert maturity
- Configured Native M365 / Azure tenant data connectors and integrated connectors for local Active Directory, on-premises services & standard Firewall(s)
- QuickStart Sentinel Workbooks and Alerts, & retention policies
- Roadmap for implementation of advanced SOAR features, event analytics, AI with Security Copilot integration and custom Playbooks for MSFT Sentinel

## Service Options

- Sentinel SOAR Advanced Capabilities, automation workbooks, analytics rules and alert enrichment
- Integration with M365 Security Copilot for Enhanced AI-Driven Security
- Integration and implementation of MSFT XDR with Defender Threat Intelligence
- Future Security Operations integration with SOC services.
- Integration with Service Now or other incident response platform or ticketing system.

## Why ivision?

### People

We promote productivity and collaboration through proactive management, clear expectations and technical expertise.

### Process

Our structured and repeatable approach is based on strategic methodology that allows you to capitalize on opportunity.

### Technology

Our proven partner ecosystem empowers us to deliver the most innovative solutions for your technology needs.

## Contact Us

Any questions on how to get started? Speak with one of our experts.

☎

✉

ivision.com