CyberOne

Microsoft Sentinel Implementation

Single-Tenant and Multi-Tenant Users

WHAT DOES THIS COVER:

CyberOne's Microsoft Sentinel Implementation begins with the initial Azure Sentinel setup and a thorough review of the current Microsoft Sentinel configuration. Following the initial setup process, our team then performs complete deployment and a comprehensive review of the existing Azure Sentinel. Specifically designed for workspace users, this solution accommodates Azure Sentinel governance, access control implementation and deployment of recommended workbooks. In addition, CyberOne's Microsoft Sentinel Implementation also includes the deployment of Microsoft Native Connectors, such as:

- Microsoft 365 Defender Connectors
- Defender for Cloud
- Azure Active Directory
- Azure Activity
- Azure Identity Protection
- Microsoft Information Protection
- Microsoft Insider Risk Management
- Office 365
- Azure DDOS
- Azure WAF
- Azure PaaS services
- Key Vault, etc. monitoring

- **Long-Term Retention**
- **Sentinel Training Session**
  - Real-world hands-on investigation
  - Scenario-based UEBA investigations
  - Advance multiple stage attack investigation using investigation graph UI
  - Automation management
- **Windows / Linux Server Logs**
  - Architect log collection
  - Using Arc with AMA agent, Log Analytics Agent, or WEF/WEC with AMA agent
  - Private link configuration (where applicable)

DELIVERABLES:

- Microsoft Sentinel base deployment
- Permissions configuration
- PowerShell script to enable rules from templates
- Native connectors ingesting
- Knowledge transfer
- Training
- Documentation on Server log collection
- Windows / Linux server logging

Gold Microsoft Partner

Microsoft

CyberOne

www.CyberOneSecurity.com