CyberOne

Microsoft Sentinel Additional Components

Third-Party Data Connectors

WHAT DOES THIS COVER:

CyberOne provides complete deployment of any third-party connector, including rule and workbook creation (where applicable).

PREREQUISITES:

- Must have a deployed and configured Microsoft Sentinel instance

DELIVERABLES:

- Logs ingesting into Microsoft Sentinel
- Analytics rules enabled
- Workbooks deployed for connector where applicable

Log Forwarder Configuration

WHAT DOES THIS COVER:

In addition to configuration of the Log Forwarder, CyberOne's service also includes guidance on architectural options, log collection and load balancing.

PREREQUISITES:

- Must have a deployed and configured Microsoft Sentinel instance

DELIVERABLES:

- Documentation on configuration
- Logs forwarding to Microsoft Sentinel

KQL Training

WHAT DOES THIS COVER:

CyberOne's KQL Training is a comprehensive training program that covers KQL query logic workflow, query building, syntax, functions, and parsing. It also includes documentation on KQL Queries and a cheat sheet for common questions.

Gold
Microsoft
Partner
Microsoft

CyberOne

www.CyberOneSecurity.com