Azure Sentinel Design

Version 2.4 Nov 2019 ©Managed Sentinel Inc.

www.managedsentinel.com

3rd Party Log Sources Special Connectors

Log Analytics API

3rd Party Threat Intel Feeds

AWS CloudTrail

Microsoft Intelligent Security Graph

Threat Intelligence

Machine Learning

Managed Sentinel

www.managedsentinel.com

Use-case Knowledgebase

Threat Intel Feeds

Log Optimization

Cloud Security Consulting

Management & Health Monitoring
Use-case development and tune-up

Microsoft Threat Experts

Azure Cloud Services

Azure Sentinel

Azure Security Center

Office 365

Azure AD

Azure PaaS

Threat Intelligence

Azure VMs

Azure Defender ATP

Native Data Connectors

Azure Apps

Log Analytics Workspace

Logs / Custom Logs / Functions / Metrics

Kusto Query Language Queries

Alerts

Workbooks

Incidents

Hunting

Playbooks

Jupyter Notebooks

Logic Apps

Azure Events Hub

Telemetry / Health Monitoring

Alerts / Reports / Tickets

Use-case Review / SIEM Usage Reports

Hosting / Non-Azure Cloud Providers

Firewall

Sentinel Agents

On-Premises

Firewall

Web Servers

Sentinel Agents

AD Domain Controllers

Sentinel Agents

Security Appliances

LAN/WAN Appliances

Syslog

Azure Sentinel Log Collector

Windows Endpoints

Sentinel Agents

Legacy SIEM

Linux Endpoints

Sentinel Agents

Information Security Office

Database/Application Servers

Custom Log Collector