Microsoft Security Stack
XDR + Azure Sentinel

Ongoing licensing costs (Customer responsibility)

Azure Sentinel log consumption (per Gb/month)
Microsoft E3/E5 licensing for M365 (per seat)
Azure Security Center licensing (per resource/month)

Initial Setup

Azure Sentinel SIEM

Infrastructure setup
Log source ingestion
Alert configuration
SOAR configuration
Optimization
Initial alert tuning
Knowledge transfer

Microsoft 365 Defender for Endpoints Defender for Identity Defender for Office 365 Cloud App Security (MCAS)

Infrastructure setup
Configuration
Integration with SIEM
Policy tuning

Managed Detection and Response (MDR)

Infrastructure setup
Integration with MDR monitoring
Incident response playbook creation
Security controls deployment

Customer's responsibilities

Provide access to infrastructure
Grant permissions/access for configuration tasks
Install agents/software on on-premises/cloud resources
Obtain REST API keys for SaaS applications
Provide expertise for custom log sources/applications
Provide feedback during tuning process and incident response playbook creation

Extended MDR - Ongoing monitoring and maintenance

Managed Azure Sentinel SIEM (8x5)

Alert tuning
New log source ingestion
Custom data connectors
Log optimization
Threat Intelligence
Support during incidents
Monthly reviews

Managed M365 (8x5)

Regular configuration tasks
SOAR
Policy adjustments
Integration with SIEM/MDR
Monthly reviews

Managed Detection and Response (24 x 7)

Alert triaging
Support during incident
Threat Intelligence
Investigation / Remediation
Escalations based on playbooks
Monthly reviews

Customer's responsibilities

Provide access to infrastructure
Provide feedback during reviews
Provide feedback during alert tuning sessions
Lead/own the incident response process
Perform investigation/remediation that require access to users/endpoints/applications
Troubleshoot endpoints and application

Other security services (Customer's responsibility)

- Governance – Risk – Compliance (CISO / Security Office)
- Business Continuity — Backup/DR
- Security Operations Center (Security Devices management – Firewall/VPN/IPS/NAC/AAA)
- Data Protection — DLP / FIM
- IDAM — Authentication/PKI
- Vulnerability & Asset Management

BlueVoyant
MANAGED SENTINEL — A BlueVoyant Company

24x7 MDR+ Co-Managed SIEM

3rd Party Risk Management Threat Intelligence

Understanding Managed Detection and Response Services – October 2020
Adrian Grigorof, Marius Mocanu – Managed Sentinel a BlueVoyant Company
High definition available at www.managedsentinel.com