Azure Sentinel

Customer Environment

CISO, Auditor(s)

Centralized view of Epic environment security posture

Azure

Threat Intelligence
Microsoft Graph Security API

Azure Sentinel Watchlists
IP Addresses, Hashes, URL, hosts

Anomaly Detection
ML Built-in Alert Rules

Microsoft Fusion
Machine Learning Correlation within Microsoft security stack

Data Enrichment

Built-in Microsoft Data Connectors

Azure AD
Azure Defender
Defender for Office 365
Defender for Identity
Office 365
Azure AD Identity Protection
Microsoft Cloud App Security
Defender for Endpoints

M365 Security Tools

Built-in Non-Microsoft Data Connectors

Load Balancer
Firewalls
VPN
EDR
DLP
DNS
MFA
PAM
WAF
Vulnerability Management
Qualys

Managed Sentinel -Custom Data Connectors

snowflake · HashiCorp Vault · Duo · Cloudflare · mimecast · aruba · DNS BIND · Cisco Umbrella

ExpressRoute

Outbound traffic restricted to Azure Log Analytics Workspace

ExpressRoute

Outbound traffic restricted to Azure Log Analytics Workspace

Azure Lighthouse

Security Alerts (via REST APIs)

Remote Management

Health Monitoring

Alerts tune-up

Log Analytics Workspace

Standard Logs
SigninLogs/AuditLogs
CommonSecurityLog
OfficeActivity
Syslog
SecurityEvent
Event
ThreatIntelligenceIndicator
SecurityAlert
Usage

Custom Logs
Custom data connectors (_CL)
Custom parsers / Placeholders

Log Management
Log retention (<2 years, 90 days free)
Customer-managed key (CMK)
Network Isolation
Access Control

Agents Management · Usage · Alerts · Dashboards · Monitoring

Kusto Query Language Queries

Alerts

Automation
Triggers
Actions
Logic Apps

Incidents
Investigations
Bookmarks
Incident Management

UEBA

Accounts
Hosts

Events
Alerts
Activities
Investigations

Threat Hunting

Hunting Scripts
Alert Templates
Azure Notebooks/mstcpy
Incident Investigations
Bookmarks/Livestream
Investigation Graph
MITRE ATT&ACK

Power BI

Azure Events Hub

BlueVoyant https://www.bluevoyant.com

Security Investigation
24x7 Managed Detection and Response
Custom Alerts

Managed Sentinel
www.managedsentinel.com

SOAR Automation
Azure Sentinel & M365 Deployment

Third Party Risk
Threat Intelligence
Cyber Forensics Incident Response
Vulnerability Management

CORE Infrastructure

SSL
Firewall
Web Servers
Sentinel Agent
Defender for Endpoints
VPN Gateway
Defender for Endpoints
Windows AD DC
Sentinel Agent
Defender for Endpoints
Defender for Identity Sensor
Syslog
Network Load Balancer
Defender for Endpoints
Windows/Linux Servers
Sentinel Agent
Servers supporting Epic infrastructure such as Monitoring Consoles, Print, Auth. Servers
SSL
Azure Sentinel Syslog Log Collector
BlueVoyant can manage this collector in customer environment

Epic

Sentinel Agent
Defender for Endpoints
Epic HyperSpace
Epic Public Web Sites:
- MyChart
- CareLink
- Citrix Web Interface
Citrix XenApp
Print Services
Epic Intranet Web Sites:
- WebBlob
- Welcome Kiosk
Epic Interconnect Services
Azure Defender
Cache Database
SSL
ExpressRoute
Centralized MMA Event Collection point
MMA Gateway

Security Investigation
Security Operation Center (SOC)

Monitoring Tools/ Dashboard

Alert Rules	Log Sources	Rule Type
MS-A701: Unusual Patient Record Accesses	Epic HyperSpace	Anomaly
MS-A702: Reconnaissance Activity Followed By Logon Attempt	Epic HyperSpace, Firewall, VPN, Active Directory, MFA	Threat Detection
MS-A703: Unusual Unsuccessful Break-The-Glass Events	Epic HyperSpace	Threat Detection
MS-A704: Unusual Successful Break-The-Glass Events	Epic HyperSpace, Active Directory, MFA	Threat Detection
MS-A705: Login Via VPN	Epic HyperSpace, Active Directory, MFA, VPN	Threat Detection
MS-A706: Anomalous Login Activity	Epic HyperSpace, Active Directory, MFA, VPN	ML Behavior Analytics
MS-A707: Unauthorized Host Logon	Epic HyperSpace, Active Directory, MFA, VPN	Threat Detection
MS-A708: Unusual Password Change Activity	Epic HyperSpace, Active Directory, MFA, MCAS	Anomaly
MS-A709: Malware Detected	M365 Defender	Threat Detection
MS-A710: Large volume of PHI data transferred in/out organization	M365 Defender	Anomaly

MANAGED SENTINEL | A BlueVoyant Company

Azure Sentinel – Epic Healthcare Integration

Epic