bluecycle

Modernize your security operations center with a Microsoft Sentinel Proof of Concept

Microsoft Security

About Us

- JP Bourget, President is Former SOAR Platform founder
- We specialize in SecOps, Data (Protection), Integrations and Threat Protection
- Emerging Microsoft Security Partner
- We partner with you and become trusted advisors
- We bring cost efficiency and effective protection to your business.

Microsoft Solutions Partner
Security

Specialist
Cloud Security
Identity and Access Management
Threat Protection

Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Modern Work

Specialist
Adoption and Change Management

bluecycle

Why choose Blue Cycle for Microsoft Sentinel?

Hyper-focused

75+

SIEM and Data Pipeline deployments since 2020

1PB+

Daily capacity deployed since 2020

Experienced

Experience across common SIEMs Cloud Providers, and 3rd party security products easing migration pains.

Increase ROI

40% Reduction

In daily ingest cost vs. self-serve implementation or proof of concept

44% Lower Cost

Reduction in total cost of operating compared to legacy solutions

Faster Time to Value

Blue Cycle's deployment methodology accelerates and optimizes a well architected deployment in weeks, not months.

Better SecOps

Detections As Code

Deploy analytics and config in Microsoft Sentinel as Code

Automate Tasks

With or without Security Copilot, we help teams accelerate daily Sec Ops tasks.

Ongoing Partner

We stay with our clients as they mature and their needs change and grow.

blue cycle

Microsoft Sentinel Proof of Concept

Click here to learn more

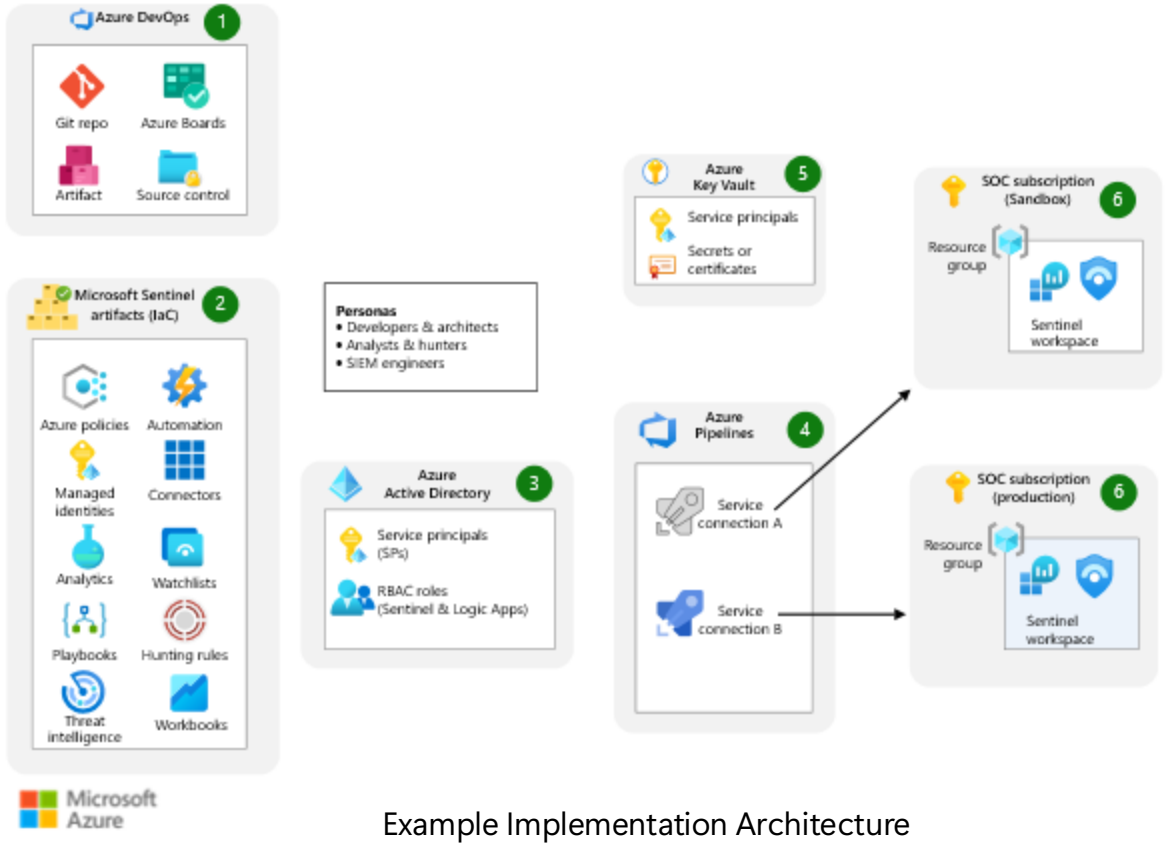
Let us help you accelerate your security modernization project through our unique service offerings.

In 30 days or less:

- Connect critical data sources to understand benefits of Microsoft Sentinel
- Experience Microsoft Sentinel with your own data
- Get clarity on the investment required to adopt Microsoft Sentinel
- Transition into a Production Deployment (add'l SOW)

Average Cost Savings:
20-40% over self serve POV/ implementation

Time to Value:
30-50% quicker than self service implementation



Example Implementation Architecture

Image Source: https://learn.microsoft.com/en-us/azure/architecture/example-scenario/devops/automate-sentinel-integration

bluecycle

blue cycle

Thank you

Microsoft Solutions Partner

Security

Specialist
Cloud Security
Identity and Access Management
Threat Protection

Microsoft Security

300+ out of the box connectors | 100+ MSSP marketplace offers | 200+ Content Hub partner solutions | 2100+ GitHub contributions

Application

- Apache HTTP Server
- Apache Tomcat
- Atlassian Confluence
- Box
- GitHub
- Jboss
- Microsoft Dynamics 365
- Microsoft Office 365
- Microsoft Teams
- Nginx
- Oracle Database
- Oracle WebLogic Server
- SAP
- Salesforce Service Cloud
- SIGNL4 Mobile
- Slack
- Snowflake
- SQL PaaS
- The Hive
- Workplace from Facebook
- Zoom

IoT

- Claroty
- Microsoft Defender for IoT

Information protection and data loss prevention

- Broadcom
- Cognni
- Digital Guardian
- Forcepoint
- NC Protect Data Connector
- Squadra Technologies

Cloud provider

- AWS Cloudtrail
- AWS GuardDuty
- AWS VPC Flow
- Azure Activity
- Azure DDoS Protection
- Azure Defender
- Azure Firewall
- Azure Information Protection
- Azure Key Vault
- Azure Kubernetes Service
- Azure Preview
- Azure Storage Account
- Google Apigee
- GCP Cloud Monitoring
- GCP DNS
- GCP IAM
- Google Workspace
- Microsoft Entra ID
- Oracle Cloud Infrastructure

Identity

- Cisco Duo Security
- Cisco ISE
- CyberArk
- ForgeRock
- Microsoft Defender for Identity
- Okta Single Sign-On
- OneIdentity
- PingFederate
- RSA SecurID
- 1 Password

IT operations

- AgileSec Analytics
- Atlassian Jira
- Cisco UCS
- Corelight
- Ivanti Unified Endpoint Management
- NXLog BSM macOS
- NXLog Linux
- Orca Security Alerts
- vArmour Application Controller
- VMwareESXi
- Contraforce

Networking

- Aruba ClearPass
- DNS
- Infoblox NIOS
- NXLog AIX
- NXLog DNS Logs
- Ubiquiti UniFi

Endpoint security

- Cisco Secure Endpoint
- CrowdStrike Falcon
- Microsoft Defender for Endpoint
- SentinelOne
- Sophos Endpoint Protection
- Symantec Endpoint Protection
- Trend Micro Apex One
- Trend Micro Vision One (XDR)
- VMWare Carbon Black

Network firewall

- Check Point
- Cisco ASA
- Cisco Firepower
- Cisco Meraki
- CloudFlare
- F5 Big IP
- Forcepoint
- Fortinet Fortigate
- Juniper SRX
- Palo Alto Panos
- SonicWall
- Sophos XG
- Windows Firewall

Email security

- Cisco SEG
- Proofpoint On Demand
- VMRay Email Threat Defender

Threat intelligence

- Recorded Future
- Reversing Labs
- RiskIQ Illuminate
- TitaniumCloud File Enrichment

Vulnerability management

- Beyond Security
- InsightVM CloudAPI
- Onapsis
- Qualys VM
- Tenableio

Web application firewall

- Azure Web Application Firewall
- Barracuda
- Citrix
- Impreva

Insider threat and user entity behavior analytics

- FalconFriday Content
- Microsoft Insider Risk Mangement

Network security

- Awake Security Arista Networks
- Cisco Stealthwatch
- Cisco WSA
- Citrix Analytics for Security
- F5 Networks (Data)
- FireEye Network Security
- Forescout
- IronNet Collective Defense
- Juniper IDP
- McAfee Network Security Platform
- Perimeter 81
- Pulse Connect Secure
- SquidProxy
- Symantec Proxy SG
- Symantec VIP
- Vectra
- Watchguard Firebox
- WireX Network Forensics Platform

Threat protection

- Abnormal Security
- Agari
- AIShield AI Security
- Akamai
- Alcide KAudit
- Alsid for AD
- Armorblox
- Automated Logic WebCTRL
- Better MTD
- Blackberry Cylance
- Contrast Protect
- Cyberpion
- Darktrace
- Deception Honey Tokens
- Delinea Secret Server
- Dev-0537 Detection & Hunting
- Elastic
- ESET Enterprise Inspector
- ESET PROTECT
- ExtraHop Reveal(x)
- Flare Systems Firework
- HYAS Insight
- Illusive Attack Management System
- Infoblox Cloud Data Connector
- Kaspersky Security Center
- Log4j Vulnerability Detection
- Lookout Mobile Threat Defense
- McAfee ePolicy Orchestrator
- Microsoft Defender XDR
- Microsoft Defender for Office 365
- Morphisec UTPP
- Proofpoint TAP
- SailPoint
- Security Threat Essentials
- Semperis Directory Services Protector
- Sophos Cloud Optix
- Symantec Integrated Cyber Defense Exchange (iCDX)
- Threat Analysis Response
- Trend Micro Deep Security
- Zimperium Mobile Threat Defense

Compliance

- CMMC
- Maturity Model for Event Log Management M2131
- NIST SP 80053
- Senserva Offer
- Sonrai Security
- Zero Trust (TIC 3.0)

Cloud security

- Barracuda CloudGen Firewall
- Bitglass
- Cisco Umbrella
- Forcepoint CASB
- Forcepoint CSG
- Microsoft Defender for Cloud Apps
- Netskope
- PAN Cortex Data Lake
- PAN Prisma
- Trend Micro Cloud App Security
- Zscaler
- Wiz