Cyber Observer and Azure Networking Integration
Unified Cloud Continuous Controls Monitoring

Challenge
Today’s challenging cybersecurity landscape offers an over-abundance of cybersecurity tools. As the number of breaches proliferates, so have the solutions and technologies designed to stop them. The state of cybersecurity is not getting easier to manage, despite enterprises and organizations worldwide spending more money than ever on new technologies and solutions.

Designed for CISOs and senior InfoSec managers (such as CIOs, C-level managers, risk officers, SOC managers and IT infrastructure personnel), Cyber Observer empowers leadership with a **unified dashboard** of their entire cybersecurity ecosystem. Cyber Observer can be fully deployed within an enterprise in a few hours, enabling easy **identification** of weaknesses, **reduction of mean-time-to-detect (MTTD)**, prevention of breaches, and advancement of your organization’s **cybersecurity posture** and **maturity**.

Solution
Cyber Observer’s partnership with Microsoft Azure enables CISOs to better manage their cybersecurity ecosystem. They receive alerts from Cyber Observer on the key aspects and issues in Azure Networking such as **Azure Firewall Policies**, **Virtual WANs**, **Load Balancers**, **WAF**, **Application Gateway**, **Network Security Groups**, **Virtual Networks configurations**, **Security Center High Status Recommendations** and more. This joint effort helps enterprises manage their Azure cybersecurity environment and **continuously monitor their cybersecurity ecosystem posture**.

KEY FEATURES
- Identifies cloud platform services that are misconfigured and malfunctioning, or missing
- Finds security gaps and provides recommendations for fixing
- Builds an ongoing security program to ensure alignment with new threats
- Uses continuous analytics to send alerts when there are deviations from normal behavior
- Automatic reporting
The integration between Cyber Observer and Microsoft Azure offers CxOs powerful and effective resilience visibility along with compliance validation and controls, to secure and monitor Azure Networking in an unprecedented manner.

Cyber Observer deploys to the corporate network automatically, in a matter of a few hours, predefined with security domains and CSC measurements to deliver three unique cybersecurity ecosystem views:

- First, it provides organizations with the best indicators of the cybersecurity tools that may be misconfigured, malfunctioning, or lacking and should be added to provide complete cybersecurity protection.
- It then reveals the security gaps that exist in each security domain and delivers continuous proactive recommendations to close these gaps.
- Finally, Cyber Observer’s machine learning analytics engine continuously calculates online measurements that represent normal behavior, and then alerts when a deviation from normal behavior is detected.

Fast and Secure Deployment

The Cyber Observer connector for Microsoft Azure Networking receives security and configuration data from the Azure Cloud Platform via an Azure Resource Manager secure REST API, using low privilege user roles, such as a reader.
Key Features & Benefits of This Integration

- **Cyber Hygiene Analysis and Reporting for Managers:** Alerts & reporting regarding Azure Networking current configuration implementation status based on the vendor’s and security standards best-practices, including security configuration issues, incidents & investigations management, admins & roles administration and more.

- **Reduced Incident Analysis Time:** Cyber Observer provides continuous alerts on deviation from normal behavior in terms of Microsoft Azure implementation and effectiveness as well as a continuous monitoring of relevant security issues in near real-time.

- **Continuous Incident Response:** Provides the CISO and other relevant managers in the organization, as well as the Azure Networking technical owners with continuous mitigation recommendation and steps to improve, for securing and monitoring Microsoft Azure implementation, effectiveness, maturity & resilience from a management perspective in an unprecedented manner.

- **Customizable Views and Reports:** Cyber Observer is highly customizable – all views and reports could be modified to the organization’s needs and structure. The integration between CyberObserver and Microsoft Azure offers CxOs a powerful effectiveness and resilience visibility, as well as compliance validation and controls.

---

**Key Use Cases**

1. **Detailed information on misconfigured and insecure Firewall policies**
   - Number of Network rules with Source Any Allow
   - Network rules with Destination Any is Allow
   - Network rules with TELNET Allow port 23
   - Number of Allow Application rules
   - Number of Policies with Threat intelligence turned off
   - Number of Azure Unsecured virtual hubs in Firewall Manager

2. **Detailed information on misconfigured and insecure WAF policies**
   - Azure WAF policies in Detection mode
   - Managed WAF rules types CDN & Front Door with Action set to allow
   - Azure WAF policies type Application Gateway with Inspect request body off
   - Azure WAF type Application Gateways without application gateways Associated
   - Azure WAF policies in status disabled

3. **Detailed information on insecure, misconfigured Virtual Networks**
   - Virtual Networks with DDoS Protection Disabled
   - Virtual Networks Subnets without Network Security group
   - Virtual Networks with diagnostic settings not defined
   - Virtual Networks with Private endpoints
   - Virtual Networks with Service endpoints
   - Number of NAT gateways

4. **Immediate alerts and detailed information on Security Center recommendations**
   - Unhealthy firewalls Recommendations with Status High
   - Unhealthy ExpressRoute circuits Recommendations with Status High
   - Unhealthy Traffic Manager Profiles Recommendations with Status High
   - Unhealthy Load balancers Recommendations with Status High
   - Unhealthy Network interfaces Recommendations with Status High
   - Unhealthy Application gateways Recommendations with Status High
   - Unhealthy network security groups Recommendations with Status High
   - Unhealthy CDN Endpoints Recommendations with Status High
   - Unhealthy Virtual networks Recommendations with Status High
About Microsoft

Microsoft Corporation (Nasdaq: MSFT) is one of the world's leading technology companies with products that include the Windows operating system, Office productivity applications, and Azure cloud services. LinkedIn, its business-oriented social network, is used by millions to make connections. Outside the office, Microsoft's Xbox gaming system is second only to Sony's PlayStation. Microsoft's customers range from consumers and small businesses to the world's biggest companies and government agencies. Geographically, Microsoft's revenue is evenly split between the US and the other countries. Microsoft founded in 1975.

About Cyber Observer

Cyber Observer is the premier critical controls monitoring (CCM) solution that simplifies the way cybersecurity tools are monitored and managed. Cyber Observer integrates hundreds of popular cybersecurity tools into a single intuitive interface that enables security and risk management executives to continuously monitor their security tools and improve their cybersecurity posture in alignment with cybersecurity, business, and regulatory frameworks. Learn more at cyber-observer.com.