Cyber Observer Technology Partners

CYBER OBSERVER

Microsoft Azure

Solution Brief

Cyber Observer and Azure Security Center 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 Security Center such as **alert and recommendations, regulatory compliance, high severity alerts types regarding detections of malicious attacks and suspicious activities** and more. This joint effort helps enterprises manage their 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

CYBER OBSERVER

Microsoft Azure

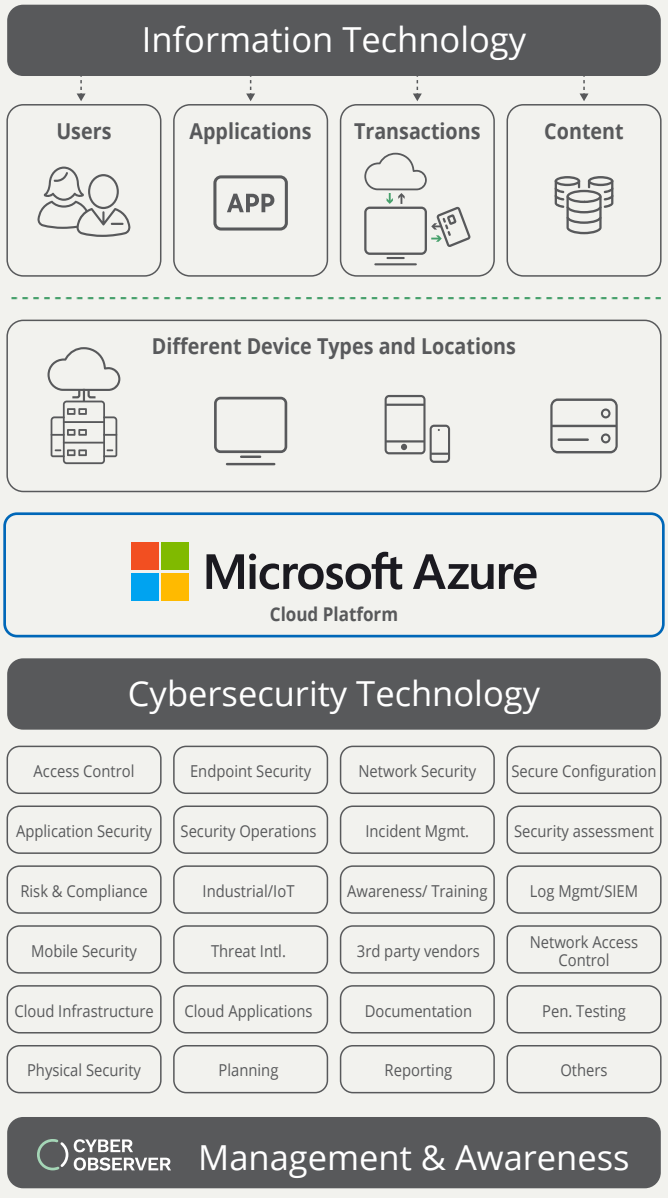
The integration between Cyber Observer and Microsoft Azure offers CxOs powerful and effective **resilience visibility** along with **compliance validation** and **controls**, to secure and monitor Azure Security Center in an unprecedented manner.

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 **missing** 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 Security Center 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.



CYBER OBSERVER

Microsoft Azure

Key Features & Benefits of This Integration

- **Cyber Hygiene Analysis and Reporting for Managers:**
  Alerts and reporting regarding Azure Security Center current configuration implementation status based on vendors' and security standards best-practices, including security configuration issues, incidents and investigations management, admins and roles administration, and more.
- **Reduced Incident Analysis Time:**
  Cyber Observer provides continuous alerts on deviation from normal behavior in terms of Azure Security Center implementation and effectiveness as well as 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 Security Center technical owners with continuous mitigation recommendations and steps to improve, for securing and monitoring Azure Security Center implementation, effectiveness, maturity and 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 Cyber Observer and Azure Security Center offers CxOs powerful effectiveness and resilience visibility, as well as compliance validation and controls.

Key Use Cases

1 Immediate alerts and detailed information on high severity alerts and recommendations

- High severity risk alerts
- High severity medium alerts
- Severity High Unhealthy Recommendations
- Number of subscriptions Azure Defender is off
- Azure Defender resource type with status off in subscriptions
- Microsoft Cloud App Security access to my data is not allowed
- Microsoft Defender for Endpoint access to my data is not Allowed

2 Immediate alerts and detailed information on regulatory compliance failures

- Number of failed regulatory compliance assessments
- Failed assessments in Azure CIS 1.3.0
- Failed assessments in Azure Security Benchmark
- Failed assessments in PCI DSS 3.2.1
- Failed assessments in ISO 27001
- Failed assessments in NIST SP 800-53 R4
- Failed assessmenta in SWIFT CSP CSCF

3 Detailed information on high severity alerts type events

- Logon from a malicious IP has been detected
- Detected Petya ransomware indicators
- Detected possible execution of malware dropper
- Digital currency mining related behavior detected
- Suspected successful brute force attack
- Behavior similar to ransomware detected [seen multiple times]
- Detected possible execution of malware dropper

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**.