

Unlock the Power of Azure Sentinel

Azure Sentinel is your comprehensive solution for advanced security monitoring, threat detection, and incident response. With a range of predefined data connectors, analytic rules, and support for User and Entity Behavior Analytics (UEBA) and MITRE ATT&CK, our Azure Sentinel deployment and administration service empowers organizations to fortify their defenses and stay ahead of evolving threats.

Data Connectors

- **Azure Active Directory:** Seamlessly integrate with Azure AD to monitor user activities, sign-ins, and access patterns.
- **Microsoft 365:** Gain insights into email, SharePoint, and OneDrive activities to detect suspicious behavior.
- **Azure Activity:** Keep an eye on Azure environment activities for secure cloud operations.
- **Microsoft 365 Defender, Microsoft Defender for Cloud, Microsoft Defender for IoT:** Elevate threat detection across various domains.

Choose from a wide selection of additional data connectors to align Azure Sentinel with your organization's distinct requirements. Our team will work closely with you to integrate data sources such as:

- **Custom Applications:** Seamlessly connect your proprietary applications to monitor their security events.
- **Third-party Security Solutions:** Integrate data from your preferred security tools for a holistic view of your environment.
- **IoT Devices:** Monitor the security of Internet of Things (IoT) devices to safeguard your infrastructure.

Predefined Analytic Rules

- **Anomalous Logins:** Detect unusual login activities that could indicate a compromised account.
- **Brute Force Attack Detection:** Identify repeated login failures as potential brute force attacks.
- **Data Exfiltration:** Detect and alert on data transfers to unapproved locations.
- **Privilege Escalation:** Identify unauthorized privilege escalations and suspicious administrative actions.
- **Suspicious File Access:** Monitor and alert on unusual file access patterns.

Additional Analytic Rules

Customized to Your Security Landscape

Tailor Azure Sentinel to your specific needs by selecting additional analytic rules that align with your organization's threat landscape. Our experts can help you define rules to address unique threats and vulnerabilities.

UEBA (User and Entity Behavior Analytics)

Azure Sentinel leverages advanced machine learning and behavioral analytics to identify abnormal user and entity activities. Detect insider threats, compromised accounts, and unusual behavior patterns across your environment. Ensure the security of your organization with UEBA.

MITRE ATT&CK Framework Integration

Azure Sentinel integrates seamlessly with the MITRE ATT&CK framework, providing you with a structured approach to understanding and countering cyber threats. Identify attack techniques, tactics, and procedures to proactively defend against adversaries.

Why Choose Azure Sentinel ?

- **Comprehensive Security:** Cover all aspects of security monitoring and threat detection with a unified solution.
- **Customization:** Tailor the platform to your organization's unique needs with additional data connectors and analytic rules.
- **Advanced Analytics:** Leverage UEBA and MITRE ATT&CK integration for proactive threat detection.
- **Scalability:** Adapt to the changing threat landscape and the growth of your organization effortlessly.
- **Expert Support:** Benefit from our experienced team's guidance throughout deployment and ongoing operations.

Don't Wait, Secure Your Future Today

Protect your organization and your clients from evolving cyber threats with Azure Sentinel. Contact us now to schedule a demonstration and discover how our Azure Sentinel services can fortify your security posture and enhance your service offerings.

Contact Information:

Email: sales@revolvesecurity.com

Website: [Revolve Security](https://www.revolvesecurity.com)