

Microsoft Azure Sentinel Implementation Services

Intelligent Security Analytics for the Entire Enterprise

For most organizations, protecting systems, data and users has never been more challenging. Cyber threats are growing rapidly in volume and sophistication, while a cloud-enabled and mobile workforce has restricted visibility and control. Now, more than ever, it is important for organizations to have full visibility across all cloud environments to detect security events and reduce attacker "dwell time."

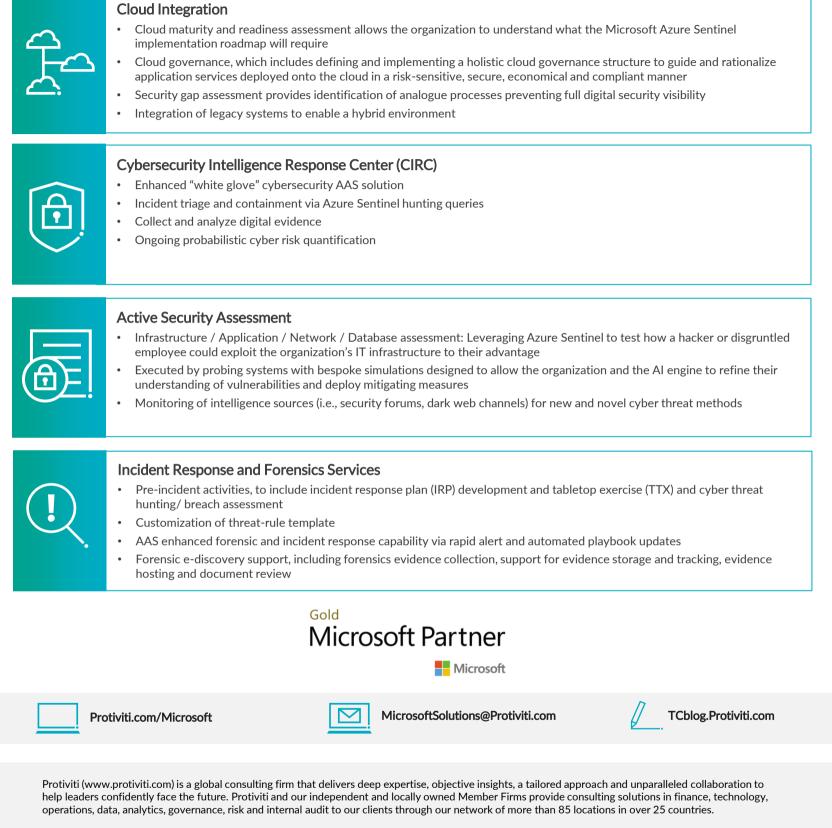
Microsoft Azure Sentinel, a cloud-native Security Information and Event Management System (SIEM) and SOAR, incorporates the power of AI to deliver intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting and threat response. It eliminates cloud security infrastructure setup and maintenance, while elastically scaling to meet your security needs, reducing IT costs.



Microsoft Azure Sentinel Capabilities

| lilii. | Data Aggregations Built on the Azure platform Fully integrated with the Azure portal to augment services; e.g., Azure Security Center and Azure Machine Learning Connectors providing real-time data integration with Microsoft and 3rd security solutions; leverages Common Event Format, Syslog or REST-API to connect to compliant data sources |
|----------|--|
| <u>Q</u> | Threat Detection Out-of-the-box rule templates enable identification and notification of threats Templates are centered on known threats, common attack vectors and suspicious-activity escalation chains Once enabled, templates can automatically search for suspicious activity |
| 678 | Threat Investigation Customizable alerts allow for the aggregation of specific evidence Easily investigate the detected threats and incident with an investigation UI Readily view the status of each incident and manage the full lifecycle of the event |
| | |

INNOVATE. TRANSFORM. SUCCEED.



Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

All referenced trademarks are the property of their respective owners. © 2020 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. PRO-0120 Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. **Protiviti**® Face the Future with Confidence