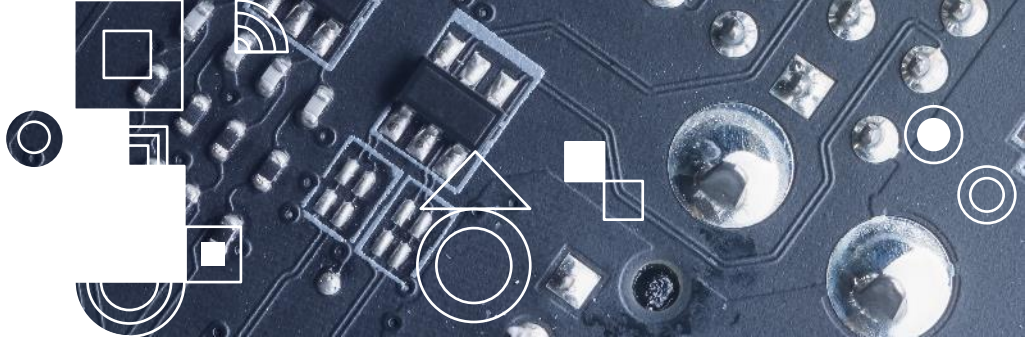
PwC and Microsoft



PwC Cyber Operations. Built for Microsoft Azure Sentinel

Despite increases in cybersecurity spending and awareness, organizations are struggling to keep pace with new threats. The average cost of a data breach is estimated at $3.92m per breach*, a 12% increase over the past five years. Expanding IT footprints, an emphasis on cloud computing, and the need to increase efficiencies further complicate an organization's ability to detect and respond to threats in a timely manner.

Cloud-native cyber operations that grow with you

PwC has teamed with Microsoft to develop managed cyber operations solutions that will rapidly integrate Azure Sentinel-driven threat detection and response (TDR) capabilities into your existing IT estate. Whether you are looking to replace your existing SIEM or implement a new cyber operations capability from the ground up, PwC and Microsoft can help you.

*Source: Ponemon Institute 2019 Cost of a Data Breach Report

A scalable cloud-native cyber operations capability

- Better predict, manage, and react to security incidents
- Move quickly to turn data into actionable information
- Tailored solutions that fit around your specific business needs
- Integrate Microsoft-native and third-party data sources to gain visibility of both cloud and on-premises systems

Expand data reach

- Consolidate multiple structured and unstructured data sources
- Integrate on-premises and in-cloud technologies, via optional custom connectors
- Scale your data consumption in line with your changing business needs via the cloud-native Azure Sentinel SIEM

Threat-driven monitoring

- Utilize custom PwC use cases, based on the MITRE ATT&CK framework
- Leverage Azure Sentinel's advanced artificial intelligence, machine learning, and threat intelligence capabilities to streamline threat detection and response

Increase efficiencies

- Continuously optimize and refine your capabilities with PwC's proven Cyber Operations team
- Develop automated response workflows and playbooks for advanced and faster triaging
- Realize cost savings via free data ingestion from Microsoft sources such as Azure Activity Log, O365 Audit Logs, and Microsoft Threat Protection products

Let PwC help you detect and respond to threats via integrated Microsoft technologies for improved visibility, speed, and response.

pwc

© 2020 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only and should not be used as a substitute for consultation with professional advisors.

Two solutions, tailored to your needs

Rapid Release

You have:

- Limited current cyber operations capabilities, or a legacy capability that is no longer fit for purpose
- A resource-constrained cyber operations team
- A heavy existing Microsoft footprint or a forward-looking Azure-first strategy

You want:

- A full-stack TDR solution that grows with your changing business and IT needs
- A cyber operations function with operationally effective processes, not just more technology

PwC and Microsoft can:

- Build a full-stack TDR platform based on Microsoft technologies
- Transition to a hybrid on/off-site managed service operated by PwC
- Perform ongoing optimization and tuning to grow in line with your requirements

Rapid Replace

You have:

- An existing cyber operations capability with multiple TDR technologies
- A legacy SIEM that lacks modern analytics, intelligence, and automation capabilities
- A heavy existing Microsoft footprint or a forward-looking Azure-first strategy

You want:

- To replace your existing legacy SIEM with a modern cloud-native alternative
- To retain your other existing TDR investments (e.g., endpoint threat detection and response software)

PwC and Microsoft can:

- Migrate your existing SIEM use cases, data sources, and customizations to Azure Sentinel
- Integrate your other TDR investments into Azure Sentinel
- Develop custom connectors for data sources not currently supported by Azure Sentinel by default

Flexible architecture

Collects data from hybrid enterprise (cloud and on-premises assets)

Analytical threat intelligence

Integrates with Microsoft's Intelligent Security Graph for unique threat intelligence and analytics

Advanced and faster triaging

Uses entity mapping and automated response workflows/playbooks

Contact us for further information

Scott Gelber, Principal
scott.gelber@pwc.com
+1 206 909 0956

Chris O'Connor, Managing Director
chris.p.oconnor@pwc.com
+1 410 200 3015

pwc | Microsoft

© 2020 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only and should not be used as a substitute for consultation with professional advisors.