Threat Detection & Response Services

Enabling you to rapidly prevent cybersecurity threats from impacting your business

Built on Microsoft Sentinel, Defender 365, Defender for IoT and Defender for Cloud

PwC's Threat Detection and Response services for Microsoft combines our expertise in engineering end-to-end M365 solutions, automation, operations and threat intelligence with the native Microsoft extended detection and response capabilities that are already included in your Microsoft license to support your ability to secure yourself from the ever-growing threat landscape.

Client challenge

The threats facing every organization are growing in volume and sophistication, overwhelming traditional threat management approaches which rely on scare and expensive skilled resources

- Cyber criminal tactics continue to evolve, getting better at evading defenses. According to the Microsoft 2022 Digital Defense Report*, it takes an average of 1h 42m for an attacker to move laterally within an organization once a device is compromised
- The cyber skills shortage will persist for the foreseeable future. According to the PwC 2021 Global Digital Trust Insights report, in the US there are 50% fewer candidates than needed in the Cyber field
- The move from on-prem, to hybrid cloud and now to multi-cloud is further accelerating the threat landscape but getting full visibility of emerging threats much harder
- Many cyber attacks are multi-pronged, targeting multiple points in an organization's infrastructure. This makes cyber attacks harder to spot unless you have a single pain of glass over an integrated toolset

How Threat Detection & Response for Microsoft can help you

1 Takes advantage of your existing investment in M365 and Azure, avoiding the need to buy additional licenses or infrastructure from third-party organizations

2 Can be custom-tailored to your specific requirements with a range of engineering, implementation and managed service options

3 Rapid Release and Rapid Replace options to get you up and running quickly with pre-built analytical rules, workbooks and Logic App automations

4 Can take advantage of our world-class threat intelligence and incident response services

Service Features

Comprehensive or Selective XDR

Choose between a full stack deployment or a more tailored approach focusing on specific elements of the Microsoft Security Stack

Full or Part-time Security Operations

Let our team operate your XDR solutions 24x7x365. Or we can supplement or complement your operations during specified hours

Can cover your entire IT and OT estate

Combine M365 XDR with our broader threat detection and response solution to monitor your complete IT and OT infrastructure

Pre-built and custom automations

Accelerate your ability to respond to threats through pre-built Logic Apps and playbooks built by PwC based on our extensive experience in Microsoft and cyber operations

Threat Detection & Response Services **in action**

Challenge: Our client had challenges facing many organizations today: how to address a growing threat landscape with tighter budget constraints and insufficient resources. Making matters worse was an existing on-prem threat management solution with alerts that lacked tuning, efficacy and coverage combined with inefficient processes driving an overstretched SOC team

Solution: In order to address the client's economic challenges without sacrificing security, PwC migrated the customer to Microsoft Sentinel, PwC then leveraged accelerators (such as our use case library and automations) to integrate the Microsoft security stack and improve the efficiency of their operations. We then layered on a 24x7 extended threat detection and response managed service

Results: The client now has a more efficient and scalable solution built around a flexible cloud-based management platform to enable them to address current and future threats. In addition, PwC's managed service addresses many of the simpler threats to their infrastructure, freeing up the client's internal team to focus on more complex incidents and other high priority tasks

Get started with Threat Detection and Response Services built on Microsoft Azure
Visit https://www.pwc.com/us/en/services/alliances/microsoft/cybersecurity.html to learn more.

Let's connect

Chris O'Connor
Managing Director
chris.p.oconnor@pwc.com

Manu Subbaiah
Director
manu.subbaiah@pwc.com

'For internal use only - not intended for further distribution'