Threat Detection & Response Services

Enabling you to rapidly prevent cybersecurity threats from impacting your business

The 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.
- The cyber skills shortage will persist for the foreseeable future.
- 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

pwc | Microsoft

The solution

Introducing

Threat Detection & Response Services

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.

pwc | Microsoft

KEY BENEFITS

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. Our solution can cover your entire IT and OT estate within a unified operating model and managed service

Threat Detection & Response Services in action

Electronics company specializing in components and enterprise computing solutions

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 economic challenges facing the client without sacrificing security, PwC migrated the customer to Microsoft Sentinel, relieving the customer of having to maintain on-prem infrastructure. PwC then leveraged accelerators (such as our use case library and automations) to integrate the Microsoft security stack (for which the client had licenses but had barely used) 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 to enable them to economically but effectively address current and future threats. They now have a flexible cloud-based threat management platform, combined with new standard operating procedures, escalation paths, and defined and reported on metrics/KPIs. What's more, 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 or other high priority tasks.

Contact

Chris O'Connor

Managing Director
chris.p.oconnor@pwc.com

Manu Subbaiah

Director
manu.subbaiah@pwc.com