Stop advanced attacks in minutes with PwC's Managed Cyber Defence

Globally sourced threat intelligence, PwC's unique detection rules, and comprehensive automation, backed by a New Zealand based team of experts.

The challenge

Being able to detect potentially malicious threats across complex environments is becoming ever more difficult as the boundaries of organisations blur.

Gaining full security visibility across your network, endpoints, servers and the cloud is near impossible. When combined with multiple toolsets, discerning real threats from noise and false positives is a time consuming activity.

How we can help

PwC's Managed Cyber Defence (MCD) is a threat-hunting, protection, detection and response service, managed 24/7. Based out of New Zealand and the UK, it is built on Palo Alto's market leading Cortex XDR and XSOAR platforms.

> Using PwC's global incident response insights, combined with threat intelligence, means we are hunting for new threats as they emerge, not once they've hit. Our automation playbooks and expert hunting skills improve threat visibility, reduce white noise and analyst workload with resolution time in minutes. Breach probability and impact is significantly reduced."
>
> **Craig Maskell**
> Partner, Cyber

Why PwC for Managed Detection and Response?

We have developed a unique set of detection rules to comprehensively protect your organisation round the clock. Combining IR insights from across our global network, threat intelligence from over 220,000 clients and our detection engineering experience, no other organisation has the global capability and expertise to integrate this level of cyber intelligence into a comprehensive MDR platform.

Market leading technology

- Cortex XDR – no other vendor achieved higher attack technique coverage than Cortex XDR in the recent MITRE ATT&CK evaluations.

Threat hunting

- MCD fuses threat intelligence, dedicated hunting skills and automation technology
- The outcome? Faster, higher detection rates, more confidence, specific advice and direction
- We provide access to our global incident response, red team and threat intelligence.

Integration

- Global incident response – bringing emerging attacker techniques from 600+ major incidents annually
- Threat intelligence – integration of threat intelligence from PwC's global network of 220,000 clients
- Defence testing – 2000 annual red/blue/purple team tests reflected in our detection capabilities.

Key benefits

Reduce analyst workload by over 50% through comprehensive automation by our SOC Bot TERRanCE, which triages all security events, provides threat enrichment, constantly rule-tunes and prioritises cases.

Stay protected with our continually evolving unique detection ruleset (currently 1000+ behavioural detection rules) powered by PwC's global threat intelligence and incident response capability. No-one else has this reach and depth of knowledge.

Our Managed Cyber Defence service can be deployed in any mode – as a standalone end-to-end detection and response service; enhancing your existing capabilities; or as an overlay service to complement traditional MSSP services.

All inclusive, monthly pricing means you won't get any surprises. Licensing, daily threat hunting, 24/7 monitoring and response, full access to all telemetry, case data and logs and real time interaction with our analysts round the clock.

Managed Cyber Defence in numbers

2,000+
Emerging attacker behaviours detected

14bn
Average daily number of events

9
Average daily cases per client

50%
Reduction in SOC staffing required for L1 / L2 analysis

3
Number of ATP groups removed through MCD powered incident response (Q1 2020)

Get in touch:

Craig Maskell
Partner | Cyber
+64 21 915 380
craig.a.maskell@pwc.com

Tum Meksikarin
Associate Director | Cyber
+64 22 163 1992
tum.x.meksikarin@pwc.com