# Effectively detect and respond to cyber attacks

**Improve your ability to detect and respond to cyber attacks using your Microsoft security solutions.**

## The challenge

To become resilient to cyber threats, organisations need to be able to rapidly and effectively detect and respond to attacks. Many organisations are not confident they can do this, uncertain about the value their existing spend has provided, and struggle with the following key questions:

What are the threats we need to be concerned about?

How do we validate we can detect these threats, and make improvements?

How do we effectively respond to alerts, and tune our false positives?

How do we get more value out of our existing investment in Microsoft security tooling?

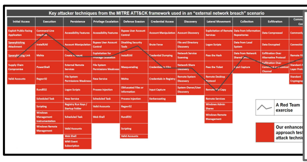
How can we automate and orchestrate our analysis of, and response to common attacks?

## Our solution

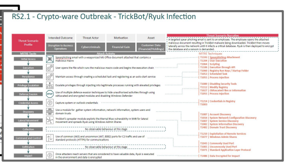
**PwC has partnered with Microsoft to help you to rapidly reorient and boost your SOC's focus, pace and effectiveness.** We bring a multi-disciplinary team in-depth knowledge of the Microsoft security solutions, using our detection and response accelerators to:

### 1 Orient your capability to your threats

Identify the threats and threat actors most likely to target your organisation, their techniques and validate your deployment of Microsoft detection capabilities and configuration.


Key attacker techniques from the MITRE ATT&CK framework used in an "external network breach" scenario

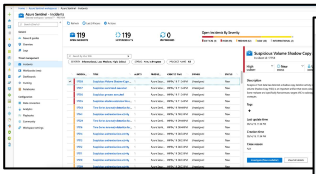
Purple Teaming Playboks


RS2.1 - Crypto-ware Outbreak - TrickBot/Ryuk Infection

Threat Modelling Library

### 2 Increase your detection coverage

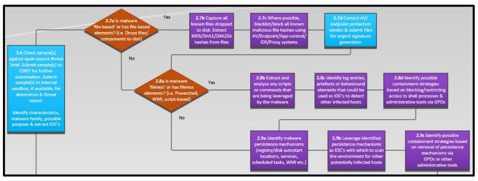
Configure Microsoft security tools to detect these techniques, by targeting the right coverage, driving focussed effort by your IT teams and developing, tuning and validating detection rules in Azure Sentinel.


Library of Detection Rules

Detection Dashboards

### 3 Reduce your time to respond

Streamline response activities, by improving the structure of security operations teams and enhancing incident response plans and playbooks.


2.6 Check sample(s) against open-source threat intel. Submit sample(s) to CSIRT for further examination. Submit sample(s) to internal sandbox, if available, for detonation & threat report.

Identify characteristics, malware family, possible purpose & extract IOC's

2.7a Is malware 'file-based' or has file-based elements? (i.e. Drops files/ components to disk)

Yes

2.7b Capture all known files dropped to disk. Extract MD5/SHA1/SHA256 hashes from files

2.7c Where possible, blacklist/block all known malicious file hashes using AV/Endpoint/App-control/ IDS/Proxy systems

2.7d Contact AV/ endpoint protection vendor & submit files for urgent signature generation

No

2.8a Is malware 'fileless' or has fileless elements? (i.e. Powershell, WMI, script-based)

Yes

2.8b Extract and analyse any scripts or commands that are being leveraged by the malware

2.8c Identify log entries, artefacts or behavioural elements that could be used as IOC's to detect other infected hosts

2.8d Identify possible containment strategies based on blocking/restricting access to shell processes & administrative tools via GPOs

No

2.9a Identify malware persistence mechanisms (registry/disk autostart locations, services, scheduled tasks, WMI etc.)

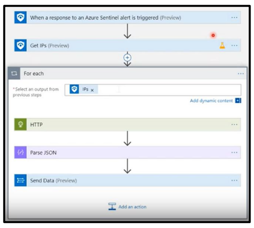
2.9b Leverage identified persistence mechanisms as IOC's with which to scan the environment for other potentially infected hosts

2.9c Identify possible containment strategies based on removal of persistence mechanisms via GPOs or other administrative tools

Response Playbooks and Processes

### 4 Optimise your use of Microsoft security tools

Configure Microsoft security tools to automate and orchestrate your response to common security threats, and free up analyst time for higher priority actions.


When a response to an Azure Sentinel alert is triggered (Preview)

Get IPs (Preview)

For each

*Select an output from previous steps: IPs

Add dynamic content

HTTP

Parse JSON

Send Data (Preview)

Add an action

SOAR Automation Flows

# Client Scenario

We recently used this approach with a FTSE 100 financial services company. They had a managed security service provider that was not effective at detecting attacks and wanted to build their own SOC based on Microsoft security tools. We helped them to:

## Target

- **Identified the threats** and threat actors targeting organisation
- **Assessed gaps** current in security tooling
- **Prioritised improvement** activities
- **Aligned to real-world threats** drawing on our experience responding to incidents.

## Improve

- **Developed requirements** and rules Microsoft's Azure Sentinel
- **Configure tools** to increase coverage, value and risk reduction
- Enabled the client to move away from their  managed security service provider

## Optimise

- **Simulated cyber attacks** to validate that improvements are effective
- **Exercised security teams** to ensure incident response processes are effective.
- Tuned tools and ensured they effectively detect threats using a Purple Team approach

# Benefits of working with the PwC and Microsoft Alliance

We combine our cross-industry experience with our in-depth knowledge of the Microsoft security solutions, to help you realise value from your investment in a cyber security platform.

Use **Microsoft Azure Sentinel** to provide a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Exploit **Microsoft 365 Defender** to coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications.

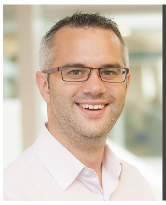
We can **bridge the gap between what you 'can do' and what you 'are doing'** bringing a full spectrum of **certified cyber specialists**, including experts in threat detection, incident response, threat intelligence, and security operations.

We are rated by Forrester as the **leading**[1] Global Cybersecurity Consulting Services provider.

We have real-world experience of defending against threats from our global **incident response practice** and our **Managed Cyber Defence** service.

[1] Forrester Wave: Global Cybersecurity Consulting Providers Q2 2019

# Your contacts



**Jonathan Cassam**
Cyber Transformation
PwC United Kingdom
M: +44 (0) 7841 803686
E: jonathan.cassam@pwc.com

**Chris Whitehead**
Cyber Transformation
PwC United Kingdom
M: +44 (0) 788 964 2782
E: christopher.j.whitehead@pwc.com

**Will Oram**
Cyber Threat Advisory
PwC United Kingdom
M: +44 (0) 7730 599262
E: will.oram@pwc.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.