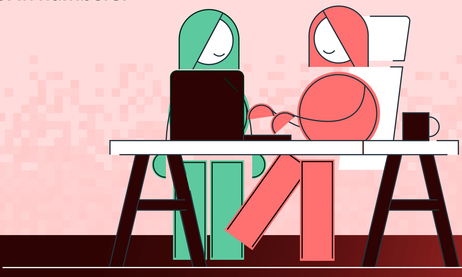
WITH secure

Spotlight on our brilliant DRT

DRT = Detection & Response Team

We talk about our DRT all the time. We love them and the work they do.

But now we can show just how good they are. In numbers!



Here's a snapshot of what they got up to in July 2023:

1304 investigations

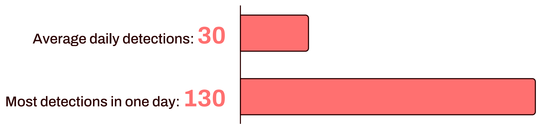
75 Elevate requests

10 penetration tests (Our clients regularly test us – and we love it!)

106 true positive detections

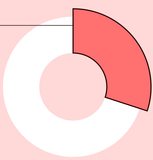
937 false positives

(We're proud of this: typical SOC numbers are 1 in 100!)



Research

The DRT spends 33% of its time on research. In July, they looked into:



EDR bypass using Freeze

Covenant C2 framework & agent capabilities

Python infostealers

Credential theft techniques using Powershell

Improving detection capability with user behaviour analytics

Users, groups and roles in Azure and AWS environments

For more info on WithSecure™ Co-Monitoring Service and how our DRT can help you, visit withsecure.com/comonitoring

WITH secure