/ MALWARE, RAT & MAAS EXFILTRATION 05D · RECURRING

Recurring Threat Hunt

€25 · Recurring · per device

> A post-incident follow-up sweep across a fleet after a confirmed MaaS or RAT incident — to catch what came back.

// DELIVERABLES

- A post-incident follow-up sweep across the fleet after a confirmed MaaS or RAT incident.
- Detection of re-infection or persistence — what came back.
- A per-sweep summary of devices showing indicators.

// EXPECTED OUTCOMES

- Confidence that a contained incident has not quietly returned.
- Early catch of persistence across the fleet.

// TIMELINE

Recurring sweep on an agreed cadence following a confirmed incident.

// METHOD OF ENGAGEMENT

Delivered as a recurring service on the Acta platform.

STEP_01 Onboarding · baseline
In-scope devices enrolled on the platform; policy baseline and cadence agreed up front.

STEP_02 Automated collection
Each cycle, device and telemetry data is collected through the platform against the baseline.

STEP_03 Review · flagging
An examiner reviews the cycle output; devices that breach policy or show indicators are flagged.

STEP_04 Cycle report
A per-cycle summary is delivered through the platform.

STEP_05 Escalation to a case
Any confirmed issue escalates into the full forensic backbone as a separately scoped investigation.

MALWARE RECURRING POST-INCIDENT