JTSECURITY MANAGED DETECTION AND RESPONSE

Detect, Response and Remediate threats before they cause distruption.

Cyber attacks are inevitable, and the threat landscape is constantly evolving. Keeping your systems protected against unknown threats can seem like an impossible task – stay ahead of attackers by taking a proactive approach to your cyber security.

What is JTSecurity Vortex Managed Detection and Response?

Vortex is JTSecuritys Managed Detection and Response (MDR) service providing proactive malware hunting, doubled up with robust, accelerated incident response capability. Using our own cutting edge technology, we significantly reduce down time from weeks to minutes. As well as detecting and removing attacks, our cyber security analysts provide answers to how and where the attack happened and took place, how to respond to the incident and how to recover your systems in the matter of minutes.

Why Now Is The Time To Take Action:

- Attackers increasingly finding ways to breach systems and move laterally within the network to evade detection. Network and log monitoring is not enough.
- Legal requirement to respond within 72 hours or face significant fines under GDPR with clarity now on what constitutes an ‘event’.
- Lack of skilled security staff and resources within IT teams with the ability to retrospectively assess ‘new’ threats quickly and see if they exist in the environment.
- Services acting as ‘alert factories’, burdening IT/security operations. Consequently, IT are missing contextual insight into specific threats targeting systems and courses of action.

Business Benefits:

- **Around the clock protection** – Providing 365 days, 24 x 7 monitoring capabilities, allows you to have piece of mind and your team to focus on your business priorities, while we focus on keeping your business safe.

- **Reduce investigation and response times down to seconds or minutes** – Our ability to monitor the endpoint, network, cloud, in near real time allows us to significantly reduce the time it takes to detect and respond to threats.

- **Stop threats before they damage the targeted system** – We include in depth malware, ransomware and exploit prevention capabilities to block most threats in real time. This uses automated behavioural and threat analysis techniques, augmented by global threat intelligence, to block many known and unknown threats in the first seconds and minutes of an attack without requiring human intervention.

- **No user disruption** – our bespoke, frictionless threat hunting agent doesn't affect day-to-day activities, ensuring there's no disruption to users at any point.

- **We won't leave you to deal with the threat alone** – We carry out pre agreed containment actions to mitigate the malicious activity. Our global incident response team are always on standby for emergency support in a large scale incident.

- **Direct engagement with our analysts** – We aim to work as an extension of your team with direct lines of communication so you can easily raise questions or request investigative support and receive answers quickly. Our monthly reporting allows your business to identify systems and aid risk analysis.

Whats Included?

Prevention

- **Multilayered malware protection** - Identifies and blocks both commodity and unknown/targeted malware before it has a chance to execute.
- **Blocking of malicious files and applications** – Executable files and office macros attempting to run in your environment are analysed in a secure sandbox and identified threats are blocked.
- **Exploit prevention –** Stops exploitation of known, zero day and unpatched vulnerabilities and protects commonly attacked programmes such as web browsers, office applications, email clients, and document readers.
- **Ransomware protection** – Block new or unknown variants of Ransomware based on behaviour before they have the chance to encrypt data and spread on the corporate network.

Detection

- **Near real time detection of threat activity** – Detection, investigation and root cause analysis of sophisticated threat activity at all stages of the attack lifecycle.
- **Backed by world class threat intelligence** – Combined with comprehensive behavioral monitoring of over 700 unique attacker tactics, techniques and procedures.
- **Mapped to Mitre ATT&CK techniques** – Our rule base is constantly updated to detect new and emerging attacker behaviours, 'fileless' malware and evasion techniques.
- **Reduce investigation times down to seconds or minutes** – Through automated analytics and context enrichment, we can significantly reduce the time between detection and response.

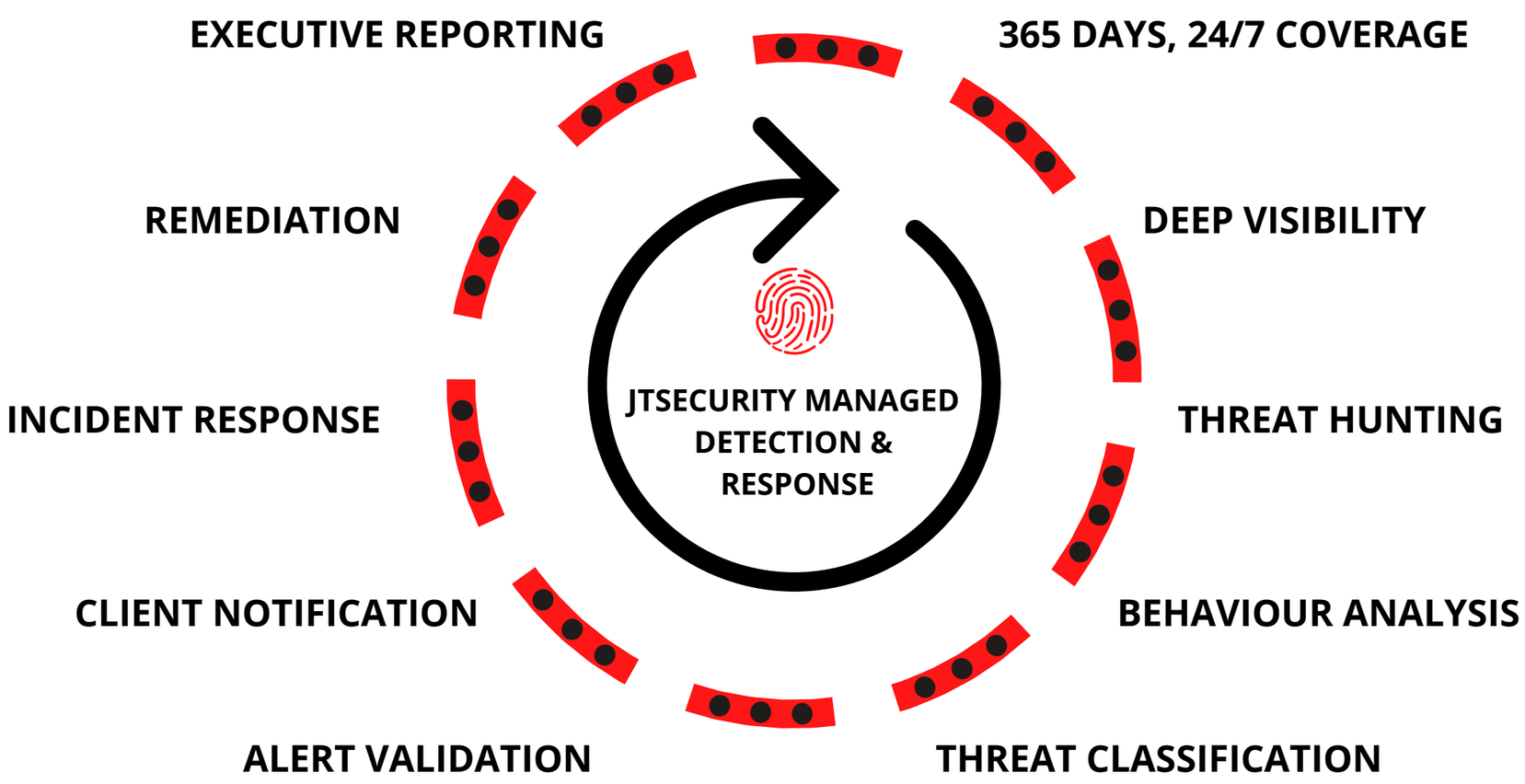
Response

- **Block malicious activity with minimal business impact** – Terminate and quarantine suspicious processes to prevent further damage, while still enabling collection of malware samples and forensic evidence.
- **Isolate attacker from the network** – Isolating suspected or known compromised machines both on and off the corporate network to protect the rest of the estate.
- **Rapid capture of forensic evidence** – Capture of malicious files and forensic evidence for further investigation, using dynamic sandbox analysis or manual reverse engineering by our dedicated threat intelligence team.

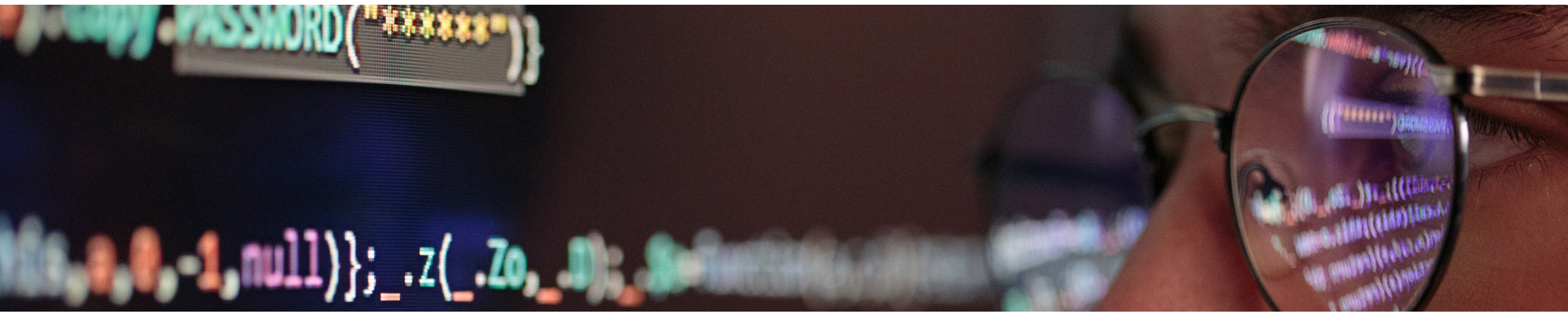
Hunting

- **Ongoing, proactive hunting** – Contextual tagging of unusual behaviours automatically creates leads for our threat hunting teams to investigate on an ongoing basis. This is complemented with targeted hunting on relevant factors such as environmental risks, changes to threat landscape, or driven by intelligence on new attack campaigns and techniques.

- **Machine learning analytics** – The critically important human context provided by our expert hunt team is augmented by advanced machine learning analytics, which can highlight subtle behavioural changes in petabytes of recorded data. Using time, entity and peer group models to baseline user, machine, process and network activity, we can quickly spot behavioural anomalies which are suggestive of highly evasive threats. This allows us to prioritise mitigation before a threat has the opportunity to turn into a breach.



Find out more about JTSecurity's Managed Detection and Response at www.jtechnical.net/vortex



Find Out More

Get in touch to discover how JTSecurity's Managed Detection and Response can help your business.

CALL US

+442033971735

EMAIL US

hello@jtsecurity.net

VISIT US

www.jtsecurity.net

johnson TECHNICAL security