Threat Informed Defence

Managed Service

DEV/NULL

Strengthen defences where adversaries strike

The cybersecurity landscape is increasingly complex, with threat actors evolving their tactics and exploiting gaps in organisational posture. Defenders also face growing regulatory pressures and the demands of hybrid environments.

Threat-Informed Defence (TID) offers a clear, evidence-driven starting point. By converting data into actionable intelligence, organisations can profile adversary behaviour and map it to Tactics, Techniques, and Procedures (TTPs), producing a structured roadmap that prioritises effort and strengthens overall security posture.

More detail

TID wraps around existing security controls to deliver measurable, adversary-aligned capability across Protect, Detect, and Respond.

- **Protect with enterprise context.** Understand the assets, dependencies, and vulnerabilities that matter most to your threat landscape, so defences are aligned to real adversary behaviours.
- **Detect with evidence-backed coverage.** Use frameworks such as MITRE ATT&CK and D3FEND to measure control effectiveness and identify detection gaps that matter.
- **Respond with speed and clarity.** Improve analysis, containment, and eradication by grounding response actions in validated adversary behaviour profiles.

The result is a prioritised, threat-led roadmap that guides Security Operations toward the highest-value defensive improvements. A Detection & Response function that understands its environment, knows the threats that matter, and applies a structured, threat-led approach to defence. This delivers:

- Relevant, current threat intelligence
- A clear understanding of enterprise-specific threats
- A prioritised TTP-driven roadmap
- Stronger detection and faster response

This enables measurable, defensible improvements aligned to real adversary behaviour.

Benefits

This service is particularly beneficial for organisations who want:

- Their teams not to be overwhelmed by noise and false positives, but want threat-led, high-fidelity detections that reduce operational burden.
- Greater adversary understanding, deep threat expertise, behaviour-aligned intelligence showing how attackers operate and what to expect next.
- Clear control effectiveness, to be able to demonstrate security maturity,
- MITRE ATT&CK and D3FEND highlighted strengths, gaps, and overlap, supporting informed investment decisions.

What’s included in the Dev/Null service?

Threat Intelligence uplift:

Enriched intelligence aligned to your industry, technologies, and adversaries. This includes automated data ingestion, threat relevance scoring, and contextual tagging to focus on what matters most.

Adversary Behaviour Profile:

A tailored profile of threat actors likely to target your organisation. Includes mapped behaviours, preferred TTPs, and known exploitation paths relevant to your environment.

TTP-Driven Roadmap:

A structured, prioritised roadmap outlining which TTPs to mitigate first, where to enhance detection, and how to strengthen defensive coverage based on intelligence, risk, and operational impact.

Enterprise Context Assessment:

Align threats to your environment by validating exposure, patch status, and relevance using asset and vulnerability data.

MITRE ATT&CK & D3FEND Profiling:

A combined analysis of adversary TTPs and defensive controls, highlighting detection gaps, control overlaps, telemetry availability, and opportunities to optimise existing tooling.

Detection Enhancements:

Creation or refinement of behaviour-led detections, response playbooks, and investigation guidance to improve accuracy, reduce analyst fatigue, and accelerate containment.

Why Dev/Null?

Responsive:

We stay flexible and adapt to your priorities, whether that means shifting focus within a project or responding to an emerging threat to provide the best security for you. Our fast-turnaround, communication, and flexible engagement models keep you moving forward without delays.

Evolving:

Continuous learning is at the core of our culture: we routinely assess, refine, and re-engineer our processes, tools, and skills to stay ahead of the threat landscape. This mindset translates into more effective, efficient, and resilient solutions for you.

Sustainable:

We design security architectures and practices that endure, focusing on long-term resilience rather than quick fixes. By embedding best practices, automating controls, and aligning with your business roadmap, we foster a culture of continuous improvement.

Established:

Our team brings deep operational experience developed across a broad range of industries and security domains, backed by proven industry and vendor certifications, and a portfolio of real-world successes. That depth of knowledge lets us solve complex problems with confidence and speed.

Enabling:

Beyond delivering services, we actively coach your staff, sharing best practices, conducting workshops, and providing hands-on training to mature your capability. The result is an empowered internal team that can sustain and expand the gains we deliver.

Actionable:

Complex cybersecurity concepts are distilled into plain language, ensuring every stakeholder, from executives to engineers, understands the risks, options, and recommended actions. This clarity drives informed decisions and smooth collaboration across your organisation.

Choose Dev/Null

Choosing the right partner to provide a TID Managed Service is crucial. At Dev/Null, we combine cutting-edge methodologies with decades of collective cybersecurity experience to deliver comprehensive services tailored to your organisation's needs. Our team brings expertise from diverse industries across all aspects of security operations - from detection and response to cyber threat intelligence and technical operations. We leverage our deep understanding of industry best practices, combined with hands-on operational experience, to provide actionable insights that drive real improvement in your security posture.

Book a conversation with one of our consultants to explore how a TID can protect you.

info@devnullsecurity.co.uk