Cyber Threat Intelligence
Managed Service

Expertise to support your defence

DEV/NULL

High-quality Cyber Threat Intelligence (CTI) separates an organisation that reacts to an attack from one that pre-empts it. Building an in-house CTI function is not only costly in terms of talent, tooling, and operational overhead, but it demands a continual learning curve that can challenge busy operational teams. By partnering with a trusted provider, you gain instant access to a seasoned threat analysis team, cutting-edge data feeds and a proven intelligence workflow, all at a fraction of the internal cost.

More detail

The Dev/Null Managed Threat Intelligence Service blends the precision of customised intelligence with the power of economies of scale. We harvest data from a broad spectrum of open-source, commercial, and client-specific feeds, then enrich it with the unique context of your environment, The result is a suite of actionable insights that fit seamlessley you're your existing SOC, SIEM, and risk-management process.

Benefits

This service is particularly beneficial for organisations who want:

- Greater internal cyber-intelligence capacity
- To understand the rapidly evolving threat landscape in a highly targeted industry
- To accelerate incident response and reduce dwell time
- Cost-effective, scalable intelligence
- To meet complex regulatory or compliance obligations

Why choose Dev/Null CTIaaS?

In a world where threat actors innovate every day, knowing *who* is targeting you, *what* they're after, and *how* they're executing attacks is the most powerful defence you can deploy. Without actionable threat intelligence, security teams react after the fact, chasing indicators of compromise that have already moved laterally or exfiltrated data. Every minute a threat actor waits to hit your network is a minute of exposure.

Dev/Null CTIaaS delivers:

- **Real-time, actionable alerts:** custom feeds that surface only the **tactics, techniques, and procedures** (TTPs) relevant to your environment, reducing noise and accelerating response.
- **Threat actor profiling and intent analysis**: deep dives into adversary groups, including motivation, capabilities, and likely next moves, enabling you to anticipate and pre-empt attacks.
- **Contextualised vulnerability mapping**: correlate emerging exploits with your asset inventory to identify the highest-impact gaps before attackers do.
- **Proactive threat hunting support**: templates, playbooks, and on-demand guidance to empower your SOC to hunt before indicators appear in your logs.
- **Secure integration & automation**: API-driven feeds that plug directly into your SOAR, SIEM, or incident-response platform, turning intel into automated actions.
- **Independently managed intelligence lifecycle**: an expert team that curates, validates, and delivers intelligence outside internal politics, ensuring timely, unbiased insights.
- **Continuous risk assessment**: regular threat landscape reports that tie emerging threats to your risk appetite, helping you prioritise resource allocation.

With Dev/Null CTIaaS, you gain a risk-driven, outcome-focused partnership that transforms raw threat data into a strategic asset, reducing dwell time, tightening incident response, and delivering measurable, business-aligned security posture.

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.

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.

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.

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.

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.

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.

Who to choose

Choosing the right partner to provide your Managed Cyber Threat Intelligence capability is crucial. At Dev/Null, we combine cutting-edge methodologies with decades of collective cybersecurity experience to deliver Cyber Threat Intelligence 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 Managed Cyber Threat Intelligence function can protect you.

info@devnullsecurity.co.uk