Continuous Threat Exposure Management

DEV/NULL

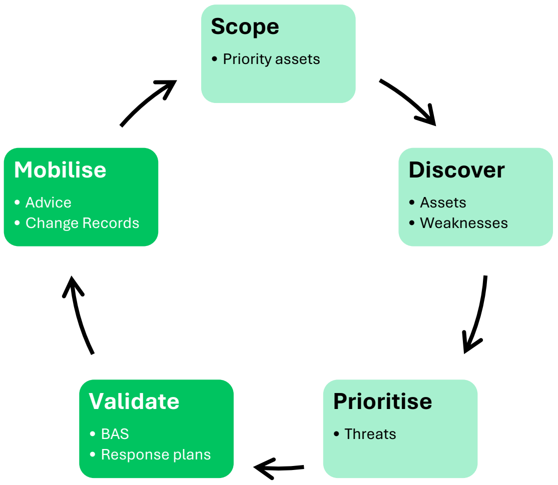
Design & Build

Continuous threat discovery and prioritisation

Continuous Threat Exposure Management (CTEM) enhances your security services to provide high fidelity prioritisation of weaknesses. These are the vulnerabilities which are confirmed to exist on your assets, have been proved to be exploitable, appear on attack paths to critical assets, and enable techniques of concern in your Threat Landscape report. Vulnerabilities identified by CTEM are the highest priority for remediation teams and take precedence over other remedial actions.

More detail

CTEM is a synergy of security capabilities: Cyber Threat Intelligence (CTI), Attack Surface Management (ASM), Vulnerability Management (VM), Attack Path Mapping (APM), Breach and Attack Simulation (BAS), and Remediation. An Intelligence-led approach, along with business objectives input, defines scenarios which represent likely adversary attack campaigns. Assets linked to the scenario become the scope of the test which identifies vulnerabilities and misconfigurations identified by your VM service and maps attack paths to associated critical assets. These paths are prioritised and tested by your BAS service or by manual penetration tests to validate exploitability and to test security controls. The outcome of this analysis is high-fidelity, high-quality prioritisation of weaknesses which are given to remediation teams for action. Findings become an input to the next scenario definition.



Scope
- Priority assets

Discover
- Assets
- Weaknesses

Prioritise
- Threats

Validate
- BAS
- Response plans

Mobilise
- Advice
- Change Records

Benefits

This service is particularly beneficial for organisations who:

- Have mature security functions including Vulnerability Management, Attack Surface Management, and Cyber Threat Intelligence
- Want to prioritise the highest risk weaknesses to efficiently reduce your threat exposure
- May have a backlog of vulnerabilities to be remediated and find prioritisation challenging.

What’s included in the Dev/Null service?

Capability analysis:

An in-depth assessment of your current cyber security capability through interview, document review, and tool review. This phase gathers all relevant data to form a complete picture of your current capability.

Service design:

A comprehensive set of documentation which includes Operating Model, Service Manual and Process Documentation, vendor selection criteria and process adoption test results.

Deployment:

Assist with the deployment of tooling, processes and testing of process adoption

Current state and Gap report:

A comprehensive analysis of the information gathered, presenting findings in an easily digestible format. This report includes maturity and capability assessment of people, process, and technology.

Purchasing:

Assistance with procuring any necessary tooling.

Ongoing support:

Dev/Null is always available to perform further reviews and improvements of your service, or to answer any questions about how to improve operation.

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 design and implement your CTEM capability is crucial. At Dev/Null, we combine cutting-edge methodologies with decades of collective cybersecurity experience to deliver comprehensive designs 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 CTEM can enhance your security services.

info@devnullsecurity.co.uk