

Sentry CTEM

Continuous Threat Exposure Management

CTEM answers the questions security teams actually have. What do we have, what is exposed, which exposures matter most, are they real, and what should we fix first?

Contents

THE SERVICE

Why Blackfoot	03
Introduction	04
How it fits together	05
Purpose	07
The CTEM model	08
The Sentry platform	09

COMMERCIAL

Service levels	19
Contact	22

THE FIVE MODULES

CVM Continuous Vulnerability Management	11
ASM Attack Surface Management	13
DM Domain Monitoring	15
BCM Breach & Credential Monitoring	16
APA Attack Path Analysis	17

Over 17 years of pragmatic, risk-based security

Formed in 2008, our aim was to bring much-needed leadership and pragmatic thinking to the world of information security and data protection. Our risk-based approach simplified security and compliance for our clients, improving their security and maximising the value of their investment. The same approach runs Sentry CTEM.

Pragmatism

We view the world in context. No client needs every service we offer. CTEM is modular for that reason: you commission the coverage your estate needs, not a bundle.

A risk-based approach, agreed with you, designed to fit your budget, need and environment.

Expertise

Our expert consultants are highly qualified, with experience across all industry sectors and a wealth of technical and operational knowledge brought to every engagement.

Delivered by expert testers, with access to the wider Blackfoot team covering a range of specialist disciplines.

Integrity

We believe in transparency, delivering honest feedback and giving our clients only what they need. Findings are presented factually, with the context required to act on them.

No inflated severities. Every finding carries the context that establishes what it means in your environment.

Assurance across the programme

Exposure management sits alongside our audit, penetration testing and advisory work, rather than being bought separately from a platform vendor.

Assessment, remediation and compliance evidence from one firm.

We take our clients' security seriously, so we do not talk openly about who we work with. Our clients include some of the world's largest brands, from supermarkets to airlines, banks to manufacturers, alongside mid-sized organisations: our offerings scale to support businesses of any size.

INTRODUCTION

A single, unified exposure management programme

Sentry CTEM is Blackfoot's comprehensive managed exposure management service. It continuously discovers, assesses, prioritises and helps support with remediating the exposures an attacker could actually use against your organisation, across infrastructure, applications, cloud platforms, your external attack surface, brand impersonation and leaked credentials. Everything is delivered and managed through Blackfoot's Sentry platform.

Sentry CTEM brings together capabilities into one programme, on one subscription using best of breed security technology.

INCLUDED AS STANDARD WITH EVERY TIER

Every finding is automatically enriched by AI with contextual risk, severity re-ranking, confidence assessment and bespoke remediation guidance. Analyst verification workflows are added on the managed tiers.

THE FIVE MODULES

-
- CVM** **Continuous Vulnerability Management.** Automated, scheduled scanning of external infrastructure, internal infrastructure, web applications and APIs, and cloud platforms.
-
- ASM** **Attack Surface Management.** Continuous discovery and monitoring of every internet-facing asset, including the ones you do not know you have.
-
- DM** **Domain Monitoring.** Detection of lookalike, typosquat and clone domains impersonating your brand.
-
- BCM** **Breach & Credential Monitoring.** Continuous monitoring for leaked credentials across breach dumps, infostealer logs and dark-web sources.
-
- APA** **Attack Path Analysis.** Correlation of findings across all modules into attacker paths, with prioritised remediation guidance.
-

HOW IT FITS TOGETHER

Five sources of findings, one prioritised list of things to fix

Every module is delivered through Sentry. Findings are enriched before they reach you, and verified on the managed tiers, then correlated so the list you work from is ordered by what an attacker could actually compromise.

STAGE 01

Discover and monitor

CVM

Infrastructure, applications, APIs and cloud

ASM

Every internet-facing asset, continuously

DM

Lookalike, typosquat and clone domains

BCM

Leaked credentials across breach and dark-web sources

APA

Correlation of findings into attacker routes

STAGE 02

> Enrich and verify

Included as standard at every tier, applied to each finding.

- ✓ Contextual risk review
- ✓ Severity re-ranking
- ✓ Confidence assessment, with a verification flag on unconfirmed findings
- ✓ Tailored remediation guidance
- ✓ Analyst verification workflows on managed tiers

STAGE 03

> Act, in Sentry

One platform for every module, with a prioritised list of actions.

- ✓ Findings ranked by genuine, exploitable risk
- ✓ Attack paths, with the choke point that breaks the most routes
- ✓ Remediation status tracking and ticketing integration
- ✓ Trend analysis showing whether exposure is reducing
- ✓ Compliance-aligned reporting and evidencing

**Thousands of findings.
The handful that actually
matter, ranked and
evidenced in a single view.**

From periodic, fragmented assessment to a continuous programme

Most organisations face the same set of visibility problems. Sentry CTEM addresses each of them.

Coverage

Technology estates change constantly. New vulnerabilities are disclosed daily, shadow IT expands, credentials leak and lookalike domains are registered. Periodic assessments are unable to keep pace.

Closed by continuous discovery and multi-domain state of the art scanning.

Prioritisation

Even where scanning exists, teams are presented with thousands of undifferentiated findings and no reliable way to identify the small number that represent genuine, exploitable risk.

Closed by AI enrichment, analyst verification and attack path analysis.

Lifecycle coverage

CTEM is not just for production. It runs across every development lifecycle, so vulnerabilities are found and fixed as you go rather than at at pre-live or after release.

Fewer issues reach production, and the ones that do cost less to fix.

Best of breed tooling

Each module draws on the technologies best suited to it, selected again by scope within each module. Premium tooling for each component, rather than one platform stretched across every problem.

You get the outcome you need, not another generic tool to run.

Five repeating stages, run as one programme

Each stage of the model maps to a capability delivered as part of the service. The cycle repeats continuously rather than resetting at each assessment.

01

Scoping

Seed assets, scan domains and the assets that matter most are defined at onboarding.

02

Discovery

Continuous discovery and scheduled scanning across infrastructure, applications, cloud and the external attack surface.

03

Prioritisation

AI enrichment applies contextual risk and severity re-ranking to every finding.

04

Validation

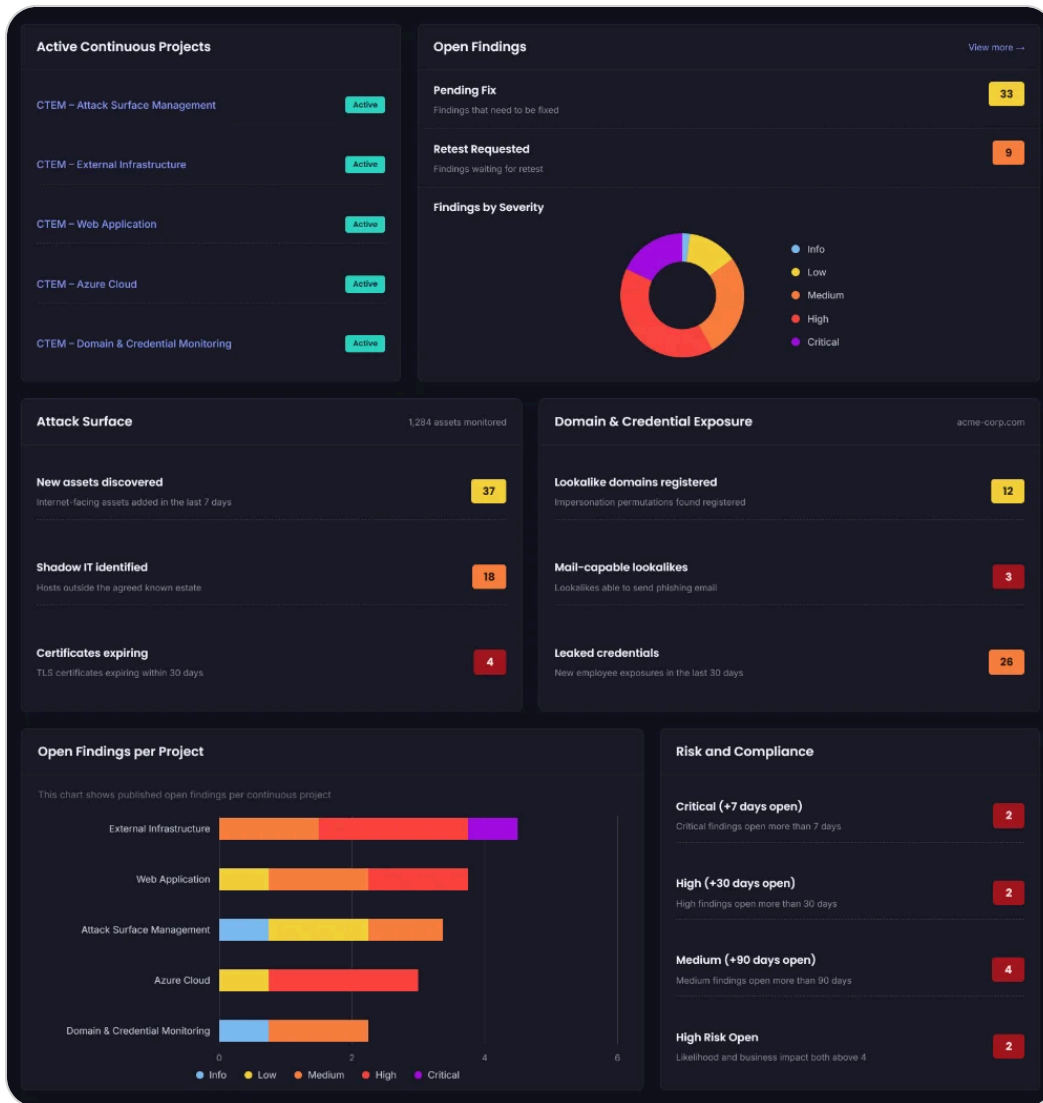
Confidence assessment, verification flags and analyst-led follow-up on our managed tiers.

05

Mobilisation

Prioritised remediation guidance, tracking, and hands-on remediation on Managed Plus.

Every module reports into one platform



Findings from every module are ingested automatically, so there is one place to see what is exposed, what has been fixed and what remains outstanding.

- ✓ Full Sentry access for all client users
- ✓ Trend analysis showing new, remediated and persisting findings over time
- ✓ False-positive marking, management and remediation status tracking
- ✓ Ticketing integration, built in
- ✓ Compliance-aligned reporting and audit evidencing capabilities



THE FIVE MODULES

Five modules, one continuous programme

The service is modular. Each module is scoped to your environment and your requirements, so you commission only the coverage your business needs.

Continuous Vulnerability Management

WHAT IT IS

Sentry CVM provides an ongoing vulnerability management capability supported by automated scanning. Scanning runs on an agreed cadence using our premium best of breed tooling, and results are ingested into Sentry. Only subscribe to the domains relevant to your estate.

HOW IT WORKS | AUTOMATED, SCHEDULED SCANNING ACROSS FOUR KEY DOMAINS

External infrastructure

Internet-facing IPs and hostnames: exposed services, open ports, known CVEs, SSL/TLS issues and authentication weaknesses, with CDN and edge-aware classification of exposure.

Web applications and APIs

DAST scanning for OWASP Top 10 vulnerability classes, authenticated scanning, and REST, GraphQL and SOAP API coverage.

Internal infrastructure

Internal ranges via a deployed scanner or agents: patch status, CVEs, Active Directory weaknesses and misconfigurations.

Cloud platforms

Configuration assessment across Azure, Microsoft 365, AWS, GCP and Oracle Cloud against CIS benchmarks: IAM, storage exposure, network security, logging and encryption. Read-only API access, no agents.

Tooling is selected according to the type of system being assessed. A single scanner applied across an entire estate leaves deficiencies, so we combine different tooling by domain to ensure the best tool is used for each job.

Continuous Vulnerability Management

WHAT IT DETECTS

- ✓ CVE-based vulnerabilities with CVSS severity ratings
- ✓ Exposed services, open ports, SSL/TLS issues and authentication weaknesses
- ✓ OWASP Top 10 vulnerability classes in web applications and APIs
- ✓ Cloud misconfiguration against CIS benchmarks
- ✓ New, remediated and persisting vulnerabilities over time, through trend analysis

WHAT YOU RECEIVE

- ✓ Initial onboarding, asset registration and scan configuration
- ✓ Automated scanning of all registered assets on the agreed cadence
- ✓ Trend analysis across scan cycles
- ✓ False-positive marking, management and remediation status tracking
- ✓ Compliance-aligned reporting for ISO 27001, PCI DSS and Cyber Essentials
- ✓ Adding or removing assets from scope
- ✓ All scan results in a single view within Sentry covering Apps, APIs, Cloud & Infrastructure
- ✓ Full client access to Sentry for all client users
- ✓ Optional integrations into your existing ticketing system as standard
- ✓ Scan scheduling, execution and platform support

The exact service shape depends on the scan domains in scope and the agreed asset count for each.

Attack Surface Management

WHAT IT IS

Sentry ASM provides an ongoing attack surface management capability supported by continuous discovery and monitoring. Discovery runs continuously rather than on a scheduled cadence, working outwards from the seed assets agreed at onboarding and updated as required.

HOW IT WORKS | FOUR CAPABILITY AREAS



Asset discovery

Continuous automated discovery of internet-facing assets including domains, subdomains, IP addresses, cloud assets and exposed services. Passive and active techniques identify assets associated with your known seed assets. New assets are flagged as they are discovered.



Certificate monitoring

Continuous monitoring of SSL/TLS certificates across all discovered assets, including expiry tracking, weak cipher detection and certificate transparency log monitoring for newly issued certificates against your domains.



Exposure monitoring

Ongoing monitoring of all discovered assets for open ports, exposed services, certificate issues, service misconfigurations and unexpected changes, with alerting on significant new or changed exposures.



Cloud asset enumeration

Discovery and monitoring of cloud-hosted assets across major providers, including internet-facing services provisioned in Azure, AWS, GCP and Microsoft 365 that may not be captured in traditional asset inventories.

Attack Surface Management

ASM

WHAT IT DETECTS

- ✓ Internet-facing assets you did not know you had
- ✓ Assets added, removed or changed since the last check
- ✓ Open ports, exposed services and service misconfigurations
- ✓ SSL/TLS certificate issues, weak ciphers and approaching expiry
- ✓ Internet-facing cloud services outside the traditional inventory

WHAT YOU RECEIVE

- ✓ Initial onboarding, seed asset registration and discovery configuration
- ✓ Continuous automated discovery from agreed seed assets
- ✓ Automatic ingestion of asset and exposure data into Sentry
- ✓ SSL/TLS certificate monitoring including expiry tracking
- ✓ Asset inventory management and ownership tracking
- ✓ Ongoing platform support and monitoring management
- ✓ Adding or removing seed assets during the subscription
- ✓ Ongoing exposure monitoring across all discovered assets
- ✓ Alerting on new, changed or removed assets and significant exposures
- ✓ Full client access to Sentry for all client users
- ✓ False-positive marking, management and asset suppression

Domain Monitoring

WHAT IT IS

Impersonating web addresses differ from the genuine domain by a single character, and an addition or omission can be used for phishing emails and imitation websites. Domain Monitoring identifies them at or near the point of registration. This allows time for notification and takedown before a phishing campaign begins, handled by Blackfoot if Managed Plus is taken.

HOW IT WORKS

- ✓ Plausible variants of the real address are generated, including characters visually identical to the original, then checked against what has actually been registered
- ✓ Registered variants are traced to their owner and host, and checked for the ability to send email
- ✓ Sites are compared against the genuine one, visually and in code, to identify clones and fake sign-in pages

WHAT IT DETECTS

- ✓ Lookalike addresses currently registered
- ✓ Those configured to send email, which commonly precedes a phishing campaign
- ✓ Those hosting a copy of the real site or a fake sign-in page

WHAT YOU RECEIVE

- ✓ Notification at or near the point of registration, with the owner, host and email capability of each variant
- ✓ Findings ingested into Sentry alongside every other module
- ✓ Takedown handled by Blackfoot on Managed Plus

Breach & Credential Monitoring

WHAT IT IS

Credentials are exposed through breaches from other organisations, malicious software on personal devices, and closed criminal marketplaces. Monitoring is tied to your own domains and runs continuously. This matters because a valid credential is a common initial access route, including where that credential originates from a personal rather than a corporate account.

HOW IT WORKS

- ✓ Logs from password-stealing software, captured directly from infected machines
- ✓ Public and private collections of breached data
- ✓ Criminal forums, messaging channels and hidden parts of the web, searched for mentions of monitored domains

WHAT IT DETECTS

- ✓ Exposed credentials tied to your monitored domains
- ✓ Exposures categorised as employee, supplier and third-party, or customer
- ✓ Corporate credentials exposed through personal accounts and devices

WHAT YOU RECEIVE

- ✓ The detail behind each exposure where available: account, exposed password, source and date
- ✓ Continuous monitoring, with alerts as new exposures are identified
- ✓ Findings ingested into Sentry alongside every other module

Attack Path Analysis

WHAT IT IS

Findings from the other modules are correlated into ordered chains showing how an attacker could move from an internet-facing entry point, through intermediate systems, to the assets identified as critical. Correlation reduces a large number of individual findings to a smaller set of remediation decisions.



HOW IT WORKS

- ✓ Critical assets are defined at onboarding
- ✓ Findings from across the modules are correlated into ordered chains, each step backed by the underlying evidence
- ✓ Paths are tracked over time as new, ongoing, resolved or changed

WHAT IT DETECTS

- ✓ Routes from an internet-facing exposure to the assets that matter most
- ✓ Choke points where one internal fix breaks the greatest number of routes
- ✓ Whether exposure is reducing, through comparison across runs

WHAT YOU RECEIVE

- ✓ A diagram of each route, suitable for technical and non-technical audiences
- ✓ Prioritised guidance distinguishing closing the entry point from cutting the choke point
- ✓ A comparison across runs showing the direction of travel

SERVICE LEVELS

Choose the level of involvement your team needs from Blackfoot

Core, Managed and Managed Plus run the same platform and the same modules. What changes is how much of the work sits with us.

Three tiers, one platform

✓ Included – Not included

FEATURE	CORE	MANAGED	MANAGED PLUS
SCANNING & DETECTION			
Automated scanning of all registered assets on agreed cadence	✓	✓	✓
All scan results in a single view within Sentry	✓	✓	✓
CVE-based detection with CVSS severity ratings	✓	✓	✓
Trend analysis (new / remediated / persisting over time)	✓	✓	✓
On-demand re-scans (outside cadence)	–	–	✓
Verification re-scans on remediation	–	–	✓
PLATFORM & WORKFLOW			
Full Sentry access for all client users	✓	✓	✓
Ticketing integration (built into Sentry)	✓	✓	✓
False-positive marking & remediation status tracking	✓	✓	✓
Compliance-aligned reporting (ISO 27001, PCI DSS, Cyber Essentials)	✓	✓	✓
Initial onboarding, asset registration & scan configuration	✓	✓	✓
Scheduling, execution & platform support	✓	✓	✓
Add / remove assets from scope during subscription	✓	✓	✓

Triage, remediation and review

✓ Included – Not included

FEATURE	CORE	MANAGED	MANAGED PLUS
AI ENRICHMENT & TRIAGE			
AI enrichment on every finding: confidence, severity re-ranking, contextual risk	✓	✓	✓
Bespoke AI remediation guidance per finding	✓	✓	✓
"Needs verification" flag on unconfirmed findings	✓	✓	✓
Follow-up on flagged findings	Client self-service	Analyst-led · AI agentic validation (roadmap)	Analyst-led · AI agentic validation (roadmap)
Verified false-positive suppression	–	✓	✓
REMEDIATION			
Remediation tracking & SLA management	–	–	✓
Hands-on remediation driving: working with your internal stakeholders to push fixes to closure	–	–	✓
Bespoke remediation metrics & reporting tailored to your organisation	–	–	✓
REVIEWS & SUPPORT			
Periodic review	–	Monthly summary / call	Monthly strategic review
Named security contact	–	–	✓
Priority support response	–	–	✓
Assisted evidence packs for audit / certification	–	–	Optional

The right tool for the job, every time. Not a general scanner stretched across everything, but best of breed, expertly paired and configured to what it is assessing.

Speak to an Expert

We will walk through your estate, the modules relevant to it, and the tier that fits how your team works. Contact us for more information today.

 0203 393 7795

 info@blackfootuk.com

 www.blackfootuk.com

OUR ACCREDITATIONS

