RAZOR'S EDGE

Continuous Threat Exposure Management

Providing continuous monitoring of your entire attack surface, combining automated scanning with expert validation to deliver actionable security insights, 24/7.

CONTINUOUS SECURITY TESTING

Razor's Edge
Continuous Security

Razor's Edge is a comprehensive Continuous Threat Exposure Management (CTEM) platform designed to identify, assess and manage your organisation's entire digital threat exposure landscape.

Unlike traditional security approaches that offer limited, point-in-time visibility, the Razor's Edge CTEM framework provides continuous monitoring and active management of security exposures, ensuring your digital assets remain secure and resilient against evolving threats, 24/7.

Validated by Experts;
Zero False Positives

Razor's Edge goes further than just detection. By combining the efficiency of automation with the expertise of human validation and exploitation.

Uncover vulnerabilities.

Prioritise threats.

Transform your security.

Continuous Security Tailored to Your Requirements

Choose from...

1. Razor's Edge The CTEM Module

Choose from 3 Service Levels (Core, Plus & Pro) to access:

- **Continuous Vulnerability Scanning**
  Razor's Edge scans your systems and applications 24/7
- **Verified & Prioritised Results**
  Each detected vulnerability undergoes a meticulous review by experienced penetration testers.
- **Security Coverage Validation**
  Your entire attack surface is mapped, ensuring no blind spots.
- **Vulnerability Mitigation Assurance**
  Assurance that mitigation measures have effectively addressed the risks.
- **Real Time Alerts**
  Receive an alert the moment a verified vulnerability is uncovered.

See next page for full details.

2. Razor's Edge CTEM & PTAAS

Gives you access to everything in the CTEM Module and the option to add:

- **Penetration Testing as a Service**
  Razor's Edge seamlessly incorporates point-in-time penetration testing into the continuous security platform.

3. Razor's Edge CTEM Module+

Gives you access to everything in the CTEM Module plus:

- **Continuous Penetration Testing**
  If annual penetration testing isn't regular enough, we give you the option to add penetration testing at a flexible frequency to your Razor's Edge module, tailored to your needs.

OPTIONAL EXTRAS

- **Cloud Configuration Review**
- **Red Team Assesssments**
- **Purple Team Assesssments**

The CTEM Module: Choose Your Service Level

FEATURE	CTEM CORE SERVICE	CTEM PLUS	CTEM PRO
Scan Regularity	Fortnightly	Weekly	Custom
Seats	3	5	Unlimited
Projects Allowed	3	5	Custom
Light Penetration Test	Via deep dive credits only	Included on each weekly scan	Included on every run
Deep-Dive Credit Allocation (bi-annual)	5	10	20
Analyst Report	Monthly Vulnerability Report	Fortnightly Vulnerability Report & Monthly Executive Summary	Weekly Vulnerability Report & Monthly Executive Summary
Executive Summary Call & Check-In	Quarterly	Monthly	Fortnightly
Priority Support SLA	2 Business Days	1 Business Day	12 hours
API Rate Limit	60 req/min	120 req/min	Unlimited
MFA Enforcement	Included	Included	Included
Data Retention	6 months	12 months	24 months
Scan Control	–	Pause / Resume	Pause / Resume
Integrations	–	Included	Included
Advanced Analytics Dashboards	–	Trend Charts & Overtime Metrics	Trend Charts & Overtime Metrics

Please note that features can be tailored to individual requirements.

THE CTEM MODULE

1. Razor's Edge **The CTEM Module**

This is Continuous Threat Exposure Management, operationalised.

The CTEM Module forms the foundation of Razor's Edge CTEM framework, systematically discovering and validating exposures across your entire attack surface to provide continuous visibility of your threat landscape.

Continuous Scanning

Razor's Edge scans your systems and applications around the clock, searching for vulnerabilities that could become entry points for attackers. It actively probes for weaknesses in various areas, including:

- Network infrastructure
- Web applications
- APIs
- Operating systems
- Databases

Verified & **Prioritised Results**

Razor's Edge transforms threat exposure management by going beyond automated discovery. Each identified exposure undergoes validation and prioritisation by experienced security analysts, aligning with the CTEM framework's emphasis on exposure context and business impact.

This expert validation ensures the accuracy of findings and eliminates false positives, allowing you to focus on genuine threats.

Comprehensive **Assurance & Coverage**

Vulnerability Mitigation Assurance

Razor's Edge provides assurance that your implemented patches and mitigation measures have effectively addressed the risks. This gives you peace of mind knowing that your defences are truly holding strong.

Security Coverage Validation

Razor's Edge meticulously maps your entire attack surface, identifying all assets and potential exposure points. This ensures no blind spots remain, leaving attackers with nowhere to hide.

Manual Exploitation
Expert Verification, Enhanced Accuracy

Our expert penetration testers conduct in depth manual exploitation of high and critical vulnerabilities, delivering comprehensive analysis of significant security threats. Through this detailed assessment, we provide actionable remediation guidance to address vulnerabilities before they can be exploited by malicious actors.

Real Time Alerts
Quickly Mitigate Risks

The moment Razor's Edge identifies a potential vulnerability, it immediately sends you an alert through secure communication channels. This ensures you can take swift action to mitigate risks before they're exploited, protecting your critical assets and maintaining business continuity.

2. Razor's Edge **CTEM & PTAAS**

Razor's Edge seamlessly incorporates point-in-time penetration testing into the continuous security platform.

Our certified penetration testers conduct thorough assessments of your specified targets, delivering comprehensive insights into your current security posture through our unified platform interface.

Using industry-standard and custom-built tools, our specialists perform detailed technical security assessments.

The testing process follows a systematic methodology, enabling our team to:

- Identify and exploit security vulnerabilities across your in-scope systems and applications

- Provide detailed technical findings and impact analysis through our centralised reporting dashboard

Integration with our platform ensures findings from periodic penetration tests are seamlessly tracked and managed alongside continuous monitoring activities.

3.

THE CTEM MODULE+

Razor's Edge **CTEM Module+**

The CTEM Module+ includes Continuous Penetration Testing

For organisations requiring enhanced exposure management, we give you the option to add penetration testing at a flexible frequency aligned with your threat landscape and risk appetite.

More Frequent Testing

For critical environments handling significant monetary transactions, organisations may require more regular comprehensive security validation.

These high risk environments require expert manual assessment to identify complex vulnerabilities that automated tools cannot detect.

With the **CTEM Module+**, our specialists will uncover security weaknesses on a frequency determined by your organisational needs.

CLOUD CONFIGURATION REVIEW

Cloud Configuration **Review**

As an additional option, Razor's Edge operatives will conduct comprehensive cloud security assessments to identify misconfigurations and security gaps across your cloud infrastructure.

Our expert team performs detailed reviews of your cloud environment, examining security controls, access management, and resource configurations across all major cloud service providers.

Our specialists combine automated tools and manual expertise to evaluate your cloud architecture against best practices and compliance standards, enabling our consultants to:

- Systematically review security configurations, focusing on critical services and high-risk components
- Identify potential vulnerabilities in cloud resource settings, IAM policies, and security group configurations

Our detailed recommendations address immediate vulnerabilities and strategic improvements to protect your cloud infrastructure.

RED TEAM ASSESSMENT

Red Team **Assessments**

Add a Red Team Assessment to your Razor's Edge package

Our Red Team operates with military precision to simulate sophisticated cyber attacks against your organisation. We design bespoke assessments that mirror real world threats by utilising the same tactics, techniques and procedures employed by criminal adversaries.

The process begins with thorough threat intelligence gathering, enabling our consultants to:

- Precisely emulate current adversary tactics targeting your organisation's critical assets and systems

- Deploy sophisticated attack scenarios based on real-world threats specific to your industry and region

Whilst this approach satisfies various compliance requirements, our Red Team's primary focus remains on delivering realistic attack simulations that truly test your security posture and incident response capabilities.

Our full range of red team assessments includes:

- Threat intelligence
- Penetration testing
- Comprehensive open-source intelligence
- Digital & physical social engineering
- APT simulations

The multiple methods used by our Red Team ensure that engagements are as realistic as possible and fully challenge the effectiveness of technology, personnel and processes.

Typically, engagements are performed on average over a 30-90 day window so that the assessment mirrors a real world intrusion as closely as possible.

Following the Red Team Assessment, Razorthorn's consultants will provide comprehensive reports outlining any vulnerabilities uncovered, including how they may be confirmed and exploited in future testing.

The activities and approaches that took place will be documented as well as observations and remedial recommendations. The report will be written in a way that it can be used to plan and develop future encounters.

A debriefing session will also be arranged to walk the company through the various breach scenarios emulated in the Red Team Assessment.

PURPLE TEAM ASSESSMENT

Purple Team **Assessments**

Add a Purple Team Assessment to your Razor's Edge package

Purple Team Assessments combine the offensive capabilities of our Red Team with the defensive expertise of a Blue Team. This collaborative approach provides real time feedback and training during simulated attacks, allowing your security team to develop more effective detection and response capabilities.

Our Purple Team exercises create a controlled environment where security teams can observe, learn from and respond to sophisticated attack techniques. This approach enables our consultants to:

- Conduct simulated attacks with immediate feedback loops to strengthen defensive controls and response procedures
- Provide hands-on training for your security team while they actively defend against realistic threats specific to your industry and region

Purple Team exercises promote collaboration between attackers and defenders. This creates a dynamic learning environment where your team gains practical experience responding to the latest attack methodologies.

Razor’s Edge
Continuous Threat Exposure Management

www.razorthorn.com

sales@razorthorn.com

0800 772 0625

4 St John’s Road
Tunbridge Wells
Kent
TN4 9NP