VERIFIED THREAT

Data Sheet 2025

Executive Summary (SCCA)

Zero False Alerts – Every alert is verified with evidence, for Zero Trust at the Network Edge

Zero False Alerts

Every alert is verified with evidence. We provide a full vulnerability exposure and detail the risks in a full log.

Always on Coverage

24/7 Red Team virtual monitoring at enterprise scale ensures continual assessment is active throughout the entire organisation.

Realtime AI Remediation

VerifiedThreat layers across existing defence setups, scales out autonomously and combines verified vulnerability testing with instant AI remediation .

Security Standards

Support for ISO 270001, SOC 2 & NIST Frameworks takes the pain out of manually recording incident and logging risk data, and automatically maps to each relevant control.

www.verifiedthreat.com/

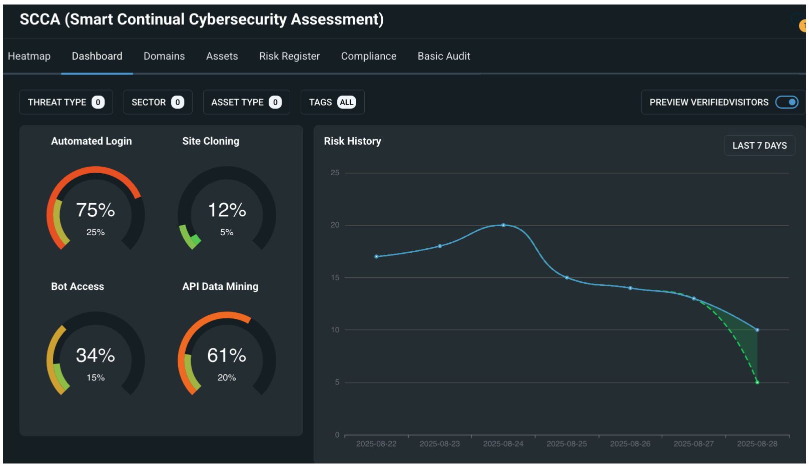
Smarter Persistent CyberSecurity Assessment (SCCA) Agents.

Board members have ultimate responsibility for the security of the company's assets and Intellectual Property, but as the notable example of Marks & Spencers has shown, it’s extremely hard to predict and manage today’s cyber-risks.

VerifiedThreat has a radically different approach and fights fire with fire. We constantly use Red Team attack tactics to verify every threat with AI-driven Red Team agents, delivering proof, not noise.

The massively scalable smart AI agents run repeatedly to expose the exploits and identify real risks across the entire enterprise.

This gives Board members and senior leadership confidence that the enterprise is protected 24/7 with robust metrics and reporting on verified vulnerabilities on a real -time basis.



Constant monitoring and building zero trust at the network edge protects the entire digital estate from later stage attacks, and ensures potential attackers are met with a robust defence.

Our AI co-pilot guides you through every step, showing the total risk surface area, and the SCCA threats that can be automatically mitigated. Business units can set their own risk profiles, along with the associated risk KPIs, so that the entire enterprise can be monitored and reported on for corporate level due diligence and risk management.

This perpetual monitoring performed by AI agents provides a huge leap forward in ensuring the enterprise is fully protected, has clear verified threat validation and is constantly monitored.

It gives the Board and senior Leadership team additional confidence that the very latest and comprehensive protection is in place for all stakeholders and ensures the highest standards of care are in place.

Please reach out to our sales team and book in a demo to see the platform in action: https://www.verifiedthreat.com

Attack Vector Chaining

Attackers can exploit weakly segmented domains to move laterally and escalate privileges. VerifiedThreat stops the attacks at the reconnaissance stage - before they can cause damage. This dramatically reduces the reconnaissance stage attacks by 70-90% and prevents more serious attack escalation in the future based on exploiting the weak defences.

Risk Insights

Track risk with non stop AI analytics. Get real-time insights to optimize threat reduction, spot the weakest links and improve your overall security governance with clear and demonstrable risk data that is 100% verified and customized to your own internal security KPIs or OKRs.

Benefits

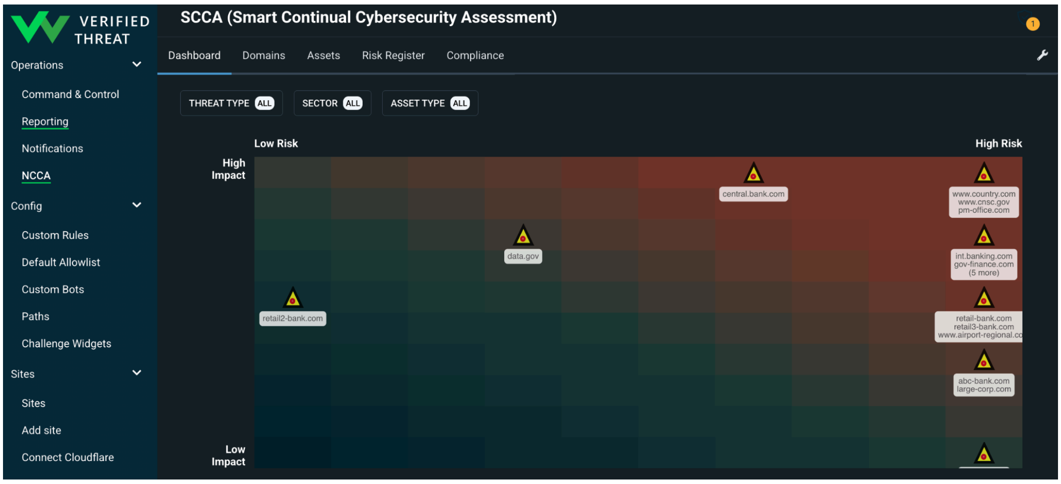
Typically our customers see an immediate decrease in reconnaissance activity which leads to 30-40% decrease in unexpected server maintenance and overhead. Benefits can be measured by setting up custom tags for each major risk area, department or risk owner, and can be reported on an enterprise-wide basis to give complete 360° visibility.

Zero Trust Framework

VerifiedThreat concentrates on the Outside In threat you would typically see from an external attack.

Reducing the threats from reconnaissance activity in the Mitre Attack Framework as shown below, stops the initial scoping in its tracks. Attackers most often use bots in the first instance to find specific vulnerabilities, and then report back, where another team can be deployed with specialist knowledge of the attack. Stopping the reconnaissance typically will result in far fewer follow-up attacks as shown.

This translates directly in less server maintenance costs, no more checking log activity and writing WAF rules that need constantly updating as threats change over time. Best of all, many of the attacks can be auto-remediated - saving valuable time checking logs and manual WAF settings.



✅ Fewer Attacks – 70–90% drop in reconnaissance activity.

✅ Lower Costs – 30–40% less unplanned server maintenance.

✅ Reduced Noise – No wasted time on false positives or log chasing.

✅ Seamless Compliance – Automated mapping to industry frameworks.

✅ Enterprise-Scale – Supports thousands of assets, domains, and environments.

Protect your enterprise with verified, continual cybersecurity assessment.
📅 Book a demo today: www.verifiedthreat.com