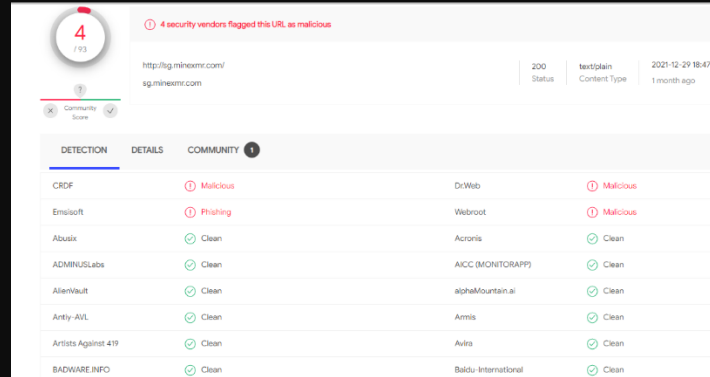


Proactive Threat Detection and Response

Specto not only monitors cyberattacks but also actively searches for Indicators of Compromise (IOCs) within a network, triggering alerts for security teams to take proactive action. This innovative approach, combined with machine learning capabilities for continuous monitoring, sets Specto apart in the cybersecurity landscape.



The screenshot shows a web interface with a red circle containing the number '4' and the text '4 security vendors flagged this URL as malicious'. Below this, there is a table with columns for 'DETECTION', 'DETAILS', and 'COMMUNITY'. The table lists various security vendors and their detection results for a specific URL.

DETECTION	DETAILS	COMMUNITY
CRDF	Malicious	DiWeb
Emis/soft	Phishing	Webroot
Abusix	Clean	Acronis
ADMINUSLabs	Clean	AICC (MONITORAPP)
AlienVault	Clean	alphaMountain.ai
Antiy-AVL	Clean	Amis
Artists Against 419	Clean	Avira
BADWARE.INFO	Clean	Baidu International



Hands-On Cybersecurity Training with Real-World Cyber Threats

The integration of Specto with the Cyberium Arena Simulator facilitates hands-on training against the most recent, real-world cyber threats. Specto promptly develops intricate scenarios for Cyberium, ensuring team involvement for extended periods, thus preparing the next generation of cyber professionals.

Detection of Zero-Day Attacks

Specto can detect zero-day attacks, which refer to cyberattacks exploiting a vulnerability unknown to the software vendors or developers, underscoring Specto's advanced capabilities and the comprehensive nature of its threat detection.

An Edge in Cybersecurity Education

With Cyberium powered by Specto, cybersecurity training becomes more real-time, responsive, and relevant than ever, enabling organizations and professionals to stay a step ahead of evolving cyber threats. Experience the future of cybersecurity training with Cyberium.

