



Gain Actionable Insights to Address Your Exposure Challenges

Proactively Discover Exploitable Vulnerabilities and Manage Exposed Digital Assets and Systems.



What X Cockpit EASM can do for you ?



Proactively Discover Exposure from Attackers' Perspectives

Identify exposures from attackers' perspectives and proactively uncover vulnerabilities and risks, unlike traditionally reactive vulnerability management.



Prioritized, Visualized Insights

Prioritize vulnerabilities visible to threat actors, assess their exploitation likelihood, and visualize external exposure correlations by risk level and digital asset categories.



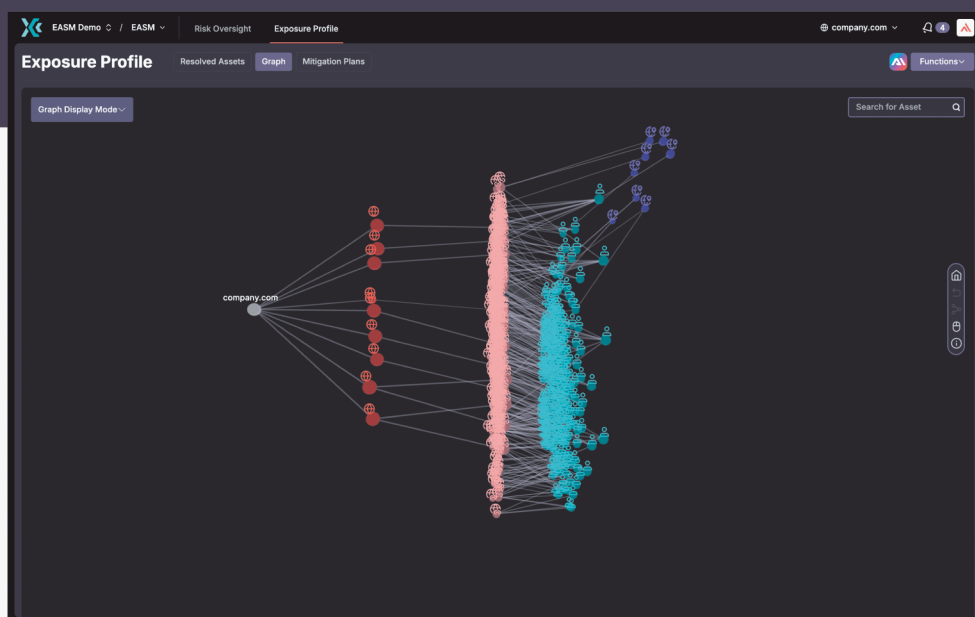
Comprehensive Threat Intelligence

Gain deep insights into dark web activities, detect compromised credentials and overlooked threats, leveraged with real-time AI reports on digital assets and supply chain vulnerabilities.



Strategic Integration and Industry Benchmarking

Motivate better investment by integrating EASM with complementary security functions, while positioning one's security posture through benchmarking with its peers in the industry.



Our Service Procedure



Discovery



Assessment



Remediation



Reporting

► Discovery

Identify, discover, and list digital assets like domains, IP addresses, and accounts.

► Assessment

Categorize and prioritize exposures based on severity, with AI-generated threat summaries and visualized event correlations.

► Remediation

Automatically merge high-severity incidents into tickets and provide mitigation recommendations.

► Reporting

Provide the security overview with status reports on asset classification, incident categories, and ticket resolutions.

CyCraftGPT

CyCraft's next-gen Cyber AI language model, designed to generate real-time AI reports on digital asset inventories, supply chain vulnerabilities, and tailored mitigation recommendations.

