Ovum
TMT intelligence | informa

On the Radar: XM Cyber simulates breaches and attacks, with prioritized remediation

HaXM platform works continually and automatically

Publication Date: 21 Feb 2018 | Product code: INT003-000050

Rik Turner

Summary

Catalyst

XM Cyber has developed a technology that identifies and exposes all attack vectors. These include lateral movement from breach points to an organization's critical assets, otherwise left undetected by security controls. It delivers automated and continual simulation of red team activity and completes the cycle by providing recommendations for how best to remediate the security holes it has identified in a corporate network.

Key messages

- HaXM is driven from a continually updated, cloud-based repository of hackers' techniques and behaviors.
- It is available either on-premises or cloud-based, with sensors deployed selectively in the customer's network to mount simulated attack campaigns.
- HaXM's virtual hacker mimics the behavior of real-world hackers, leveraging misconfigurations, user activity, collected credentials, and vulnerabilities to gain control of the network and access organizational assets.
- Based on its findings, the system exposes all attack paths and generates reports for the customer with recommendations for remedial action based on the criticality of the attack vector.

Ovum view

The shortcomings of both the vulnerability management and penetration ("pen") testing approaches, not to mention the limitations of red team security initiatives, create the market opportunity for XM Cyber, and should enable it to build a customer base in the enterprise and midsize market segments.

Recommendations for enterprises

Why put XM Cyber on your radar?

XM Cyber technology, which bears the product name HaXM, monitors a customer's security posture automatically by simulating attack scenarios, then exposes all attack paths and proffers concrete recommendations for how best to remediate any problems it has found. This makes it a compelling option for any enterprise planning to move beyond traditional pen testing, red teams, and/or vulnerability management.

Highlights

HaXM consists of three components:

- A comprehensive database of hacking methods that resides in the company's infrastructure and is continually updated by the researchers at XM Labs in Israel.

- A server, the "brain" of the product (either on-premises or cloud-based), which communicates with sensors deployed in the customer's environments, be it their LAN, data center, or cloud infrastructure. The vendor recommends that it should be able to track upwards of 10% of the customer's endpoints (including servers) to give a representative sample across the estate. HaXM identifies security holes and risks associated with IT practices, as well as computing all other potential vectors of attack in the environment, and simulates attacks to determine how a real threat actor could compromise the customer's critical assets, given the customer's current security posture – how easy it would be for someone to access the production environment or key assets within it, hijack privileged credentials, perform lateral movement within the infrastructure, or contaminate assets, for instance.
- Based on the findings from these simulations, it generates reports to guide the customer's remediation actions, providing both standard best practice and actionable suggestions with differing degrees of harshness (e.g. one option could be the complete removal of write access from a given application, while another might be to remove it only from a particular file).

A key concept in gauging the criticality of the threat vectors computed by HaXM is what the company terms "network superiority." XM Cyber defines a threshold of 80% of the sensors it has placed on the customer's infrastructure, and if a simulated attack campaign has been able to access that threshold, the vendor considers that it has achieved network superiority and remediation should therefore be prioritized.

Background

XM Cyber was founded in 2016 by former members of the Israeli intelligence community: CEO Noam Erez and CTO Boaz Gorodissky, both of whom held executive positions within that community, and the company's chairman, Tamir Pardo, who is a former head of Mossad (the Israeli secret service).

The company was formed to address what its founders perceived as a gap in the market that is not covered by existing technologies, i.e. vulnerability assessment/management and pen testing tools. They saw that both pen testing and red team approaches are not only manual (i.e. not automated), but also sporadic rather than continuous, while vulnerability management tended to result in random rather than systematic remediation and lack the most crucial aspect, shadow IT/user activity. They also sought to craft a service that could be made available in an ad hoc, on-demand manner, rather than a software product that would add to management overhead.

Current position

XM Cyber already has several paying clients in its target enterprise segment, particularly in the financial sector.

The pricing model for the product is an annual fee for the software, the size of which depends on the number of endpoints/size of the network that the system will be protecting.

In terms of its competitive landscape, XM Cyber comes up against three sets of technology vendors. The first set comprises vulnerability assessment and management vendors such as Qualys, Tenable, and Rapid7, but the company argues that

- vulnerabilities are only a small subset of a hacker's arsenal
- such tools ignore attack methods that leverage user activity

- they often overlook shadow IT
- they do not address the need for prioritized remediation suggestions.

The second set comprises vendors of pen testing services and tools, such as Metasploit, Nessus Vulnerability Scanner, Wireshark, and Kismet, many of which are freely available and open source. In relation to these products, XM Cyber argues that

- they do not scale well to large networks
- their results lose relevance quickly as the corporate network evolves, i.e. they do not keep pace with changes in the architecture, systems, and configurations
- continuously and manually identifying and prioritizing potential attack vectors is simply not feasible.

Many companies take pen testing as a service from the likes of HP Fortify, IBM Security AppScan, Veracode, Coverity, and Core Security. In this context, XM Cyber argues that the lack of highly skilled professionals often makes for only mediocre testing results. Of course, larger and more advanced enterprises will go further, forming a so-called red team of internal pen testers, but that is an expensive option that is not available to all sizes of company and provides limited scenarios (because they are human-driven tests) and at a certain point in time.

The third, still-emerging set comprises vendors of breach and attack simulation, for example SafeBreach, Verodin, and AttackIQ. XM Cyber is set apart from the competition:

- It takes a new approach beyond security control validation which consists of checking constantly the ability of a hacker to get access to the customer's critical assets using all the methods: activating exploits on vulnerabilities, shadow IT, misconfigurations, human behaviors and mistakes, and so on (exactly like a cyber attacker in the real world).
- It provides a unique solution that identifies all the attack vectors to an organization's critical assets, otherwise undetectable, by simulating continuously and automatically company-wide attack scenarios, while working safely in an organization's network.
- It exposes real vectors of attack from the breach point to the customer's assets, and provides a concrete and prioritized actionable remediation plan.

Data sheet

Key facts

Table 1: Data sheet: XM Cyber

Product name	HaXM	**Product classification**	Breach and attack simulation
Version number	1.0	**Release date**	January 2018
Industries covered	All	**Geographies covered**	North America, Western Europe, Australia, Singapore, Israel
Relevant company sizes	Enterprise, midsize	**Licensing options**	Yearly subscription per network size
URL	http://www.xmcyber.com	**Routes to market**	Direct, channel, system integrators
Company headquarters	Herzliya, Israel	**Number of employees**	30

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

On the Radar: Cymulate provides breach and attack simulation from a single agent, INT003-000008 (January 2018)

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum
TMT intelligence | informa

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo