XM CYBER®

Introducing the world's first breach and attack simulation for hybrid cloud environments

Gain Full Visibility into Potential Attacks Across Amazon Web Services (AWS) Environments

Consider all the components required to build a successful AWS infrastructure: virtual machines, databases, connections to multiple services, as well as security roles and policies. There are many opportunities to make mistakes or misconfigure accounts and permissions. The result might expose your critical data to a wide audience outside your network. XM Cyber helps you understand your use of AWS from attacker's perspective.

As more and more data are migrated to the cloud, new risks emerge making it critical for companies to assess their risk posture and understand how attackers can operate within their cloud environment. Organizations relying on the cloud must now understand how their new hybrid environment can be attacked from on premise devices that link to cloud data.

If you are assessing your on-prem risk separately from your cloud risk, you have no way of knowing what risks they pose to each other. XM Cyber closes the loop between on-prem and cloud risk assessment via automated, advanced breach and attack simulation.

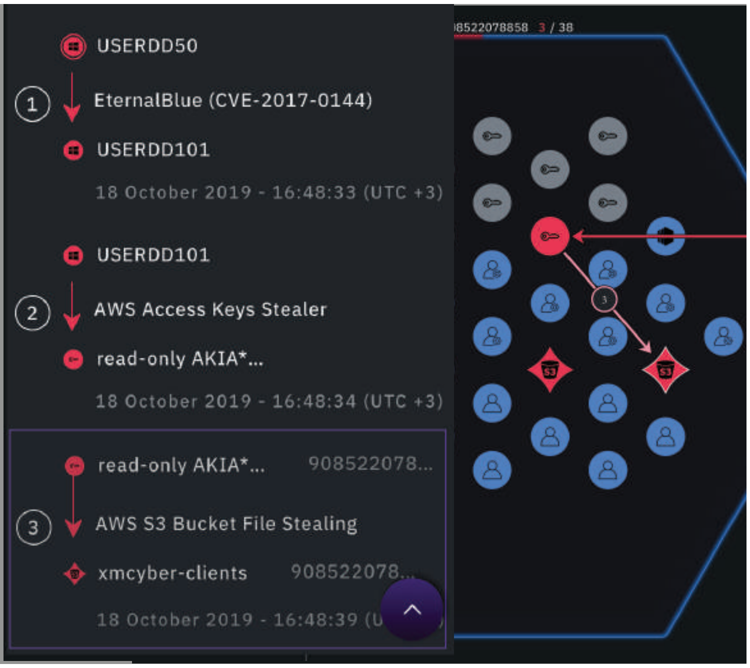
The XM Cyber platform audits AWS configurations via AWS API and uses that information to calculate different attack vectors. By simulating attacks on an organization's AWS infrastructure, it is possible to find misconfigurations leading to risks such as IAM privileges escalations, access token theft or leveraging of the Cloud Instance Metadata API to pivot across the cloud.

XM Cyber reduces cybersecurity risk by continuously simulating advanced persistent threats against an organization's critical assets, identifying security gaps, and prioritizing remediation. The platform enables users to operate as an automated purple team, combining red and blue teams' processes to ensure that organizations are always one step ahead of the attack.

Implementing in an AWS environment is a simple process requiring less than an hour.

Secure your AWS Migration

Most organizations are still in migration mode. It is critical for organizations to deploy XM Cyber while they are migrating to the cloud, not just afterwards. Attacks can happen during migrations, and mistakes that happen throughout the migration process must be identified and fixed. The benefit is you can confidently build your AWS infrastructure in a fully secure manner that will not require a re-architecture at a later date.



USERDD50

1 EternalBlue (CVE-2017-0144)

USERDD101

18 October 2019 - 16:48:33 (UTC +3)

USERDD101

2 AWS Access Keys Stealer

read-only AKIA*...

18 October 2019 - 16:48:34 (UTC +3)

read-only AKIA*... 908522078...

3 AWS S3 Bucket File Stealing

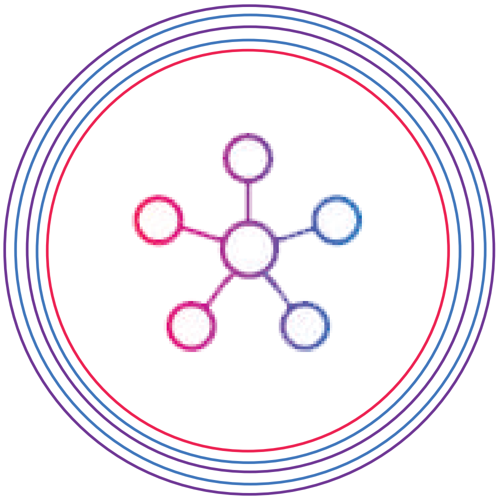
xmcyber-clients 908522078...

18 October 2019 - 16:48:39 (U

Summary

The XM Cyber platform is now the first BAS solution that can simulate attacks on Amazon Web Services (AWS). XM Cyber provides a hyper-realistic BAS solution: an advanced persistent threat (APT) automated and continuous simulation and remediation platform. XM Cyber allows users to see their network from the eyes of the attacker, running continuously 24/7 to find and show all the hidden attack vectors that can go under the radar of most protective measures.

XM Cyber is the only BAS provider to address the sole crucial question for enterprises – Are my critical assets really secure on-prem and in the cloud?



Key Benefits

- Identify security gaps in AWS implementations resulting from mistakes, misconfigurations and poor IT hygiene.

- Apply during migrations to eliminate security risks throughout the process

- Identify hybrid attack possibilities where on premise and cloud infrastructure connect
- Run 24/7 continuous attack simulations to spot security issues as they happen

- Protect critical assets stored in AWS by identifying every attack vector available to hackers

- Prioritized remediation optimizes resources

About XM® Cyber

XM Cyber provides the first fully automated breach and attack simulation (BAS) platform to continuously expose attack vectors, from breach point to any organizational critical asset. This continuous loop of automated red teaming is completed by ongoing and prioritized actionable remediation of security gaps. In effect, XM Cyber operates as an automated purple team that fluidly combines red team and blue team processes to ensure that organizations are always one step ahead of the attack. XM Cyber has already received over 20 industry awards, including being recognized as a “Technology Pioneer” by the World Economic Forum. XM Cyber’s customers include leading financial institutions, critical infrastructure organizations and manufacturers across North America, Europe, and Israel.

XM Cyber was founded by the highest caliber of security executives from the elite Israeli intelligence sector. Together they bring a proven track record in both the offensive and defensive cybersecurity domain. The company is headquartered in Israel and has offices in the US, UK and Australia.