GAIN FULL VISIBILITY INTO POTENTIAL ATTACKS ACROSS AMAZON WEB SERVICES (AWS) ENVIRONMENTS

By Raz Kotler, VP Customer Operations, XM Cyber

THE AWS SECURITY CHALLENGE

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 the 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.

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.

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.

KEY BENEFITS FOR SIMULATED ATTACKS ON AWS

- Implementation of standard IT networks into operational networks
- Poor IT hygiene (changing permissions and forgetting to switch them back)
- Vulnerabilities related to data maintained on third party supplier/customer networks
- Improper connection and USB errors that can jeopardize even air-gapped networks

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?

"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."

ABOUT XM CYBER

XM Cyber was founded by security executives from the elite Israeli intelligence sector.

XM Cyber's core team is comprised of highly skilled and experienced veterans from the Israeli Intelligence with expertise in both offensive and defensive cyber security.

XM Cyber has developed more than 15 patented technologies based on a proprietary set of algorithms that enable the continuous and automatic simulation of a hacker's techniques and methods.

RAZ KOTLER

Mr. Kotler brings 10 years of experience in Operations Management, including Customer Success, DevOps and IT. Prior to XM Cyber, Mr. Kotler was VP Operations and Customer Success at Deep Instinct, and managed all technical customer-facing activities, from pre-sales and campaign establishment to post-sales, customer satisfaction, re-engagement and escalations. He started his career at Check Point Software Technologies, where he initiated and led customer success processes and activities worldwide.