ThreatModeler Launches Integrations to Simplify Identity and Access Management (IAM) Aligned with Least Privilege Model (LPM) and Identify Vulnerabilities

Users Enforce Governance Based on Least Privilege Access Permissions and Vulnerability Intel Management

ThreatModeler announces its platform integration with AWS IAM and AWS Systems Manager (SSM). With ThreatModeler, Cloud Security Architects (CSAs) can now simulate and manage access to data assets stored in the cloud. AWS SSM lists an inventory of software installed on your servers. ThreatModeler identifies vulnerabilities tied to each software application listed. These vulnerabilities are security exposures and weaknesses that can increase risk.

Policy language dictates AWS access based on who is allowed to access what resources under which conditions. At enterprise scale, this poses a challenge with thousands of users working with numerous applications – each needing permissions. The highly distributed nature of cloud computing and microservice-based applications adds to the complexity of access management at scale. CSAs spend most of their time guessing permissions without having a clear visibility on the impact. Frequent technology changes, and fluctuations in individual roles and responsibilities, add to that uncertainty, slowing down the process.

ThreatModeler enables CSAs to leverage a simulated environment to make real-time access management decisions. CSAs visualize IAM policy changes to gain an understanding of how the changes impact the AWS environment. CSAs can review the risk information, flag and act upon access policies that haven't been used in while.

ThreatModeler provides CSAs with the vulnerability data tied to software used, which allows them to push threats as individual stories or tasks for mitigation. This is a proactive (implement security controls on the servers) vs. reactive (remediating after a vulnerability is exploited) approach.

"Identity and access management has always been challenging for cloud security architects. ThreatModeler is committed to helping solve this challenge – from designing the architecture to post deployment," said Archie Agarwal, CEO and Founder of ThreatModeler. "As the need increases for a single platform that gives an enterprise view of cloud security, ThreatModeler helps to bridge the need."

"ThreatModeler's new features have enabled us validate our architecture post deployment and secure our assets, by making educated, faster access permissions decisions. Integrations with our CI/CD tool set seamlessly allows us to translate our designs into requirements in the development process," said Tom Holodnik, principal security architect at Intuit.

FAQ

Q. What are you launching today?

A. We are launching a ThreatModeler feature integration with AWS Identity and Access Management (IAM) and AWS Systems Manager (SSM). <<ThreatModeler IAM Analyzer>> helps CSAs to easily audit their over-permissive IAM policies and unused roles. Also, ThreatModeler gives CSAs an aggregated view of the assets on their AWS EC2s and the vulnerabilities that come with them.

Q. How does the ThreatModeler integration with AWS IAM help me to achieve LPM?

A. Within access management, a challenge is to keep roles, users and groups updated, while controlling access based on LPM and reviewing permissions on a regular basis. ThreatModeler addresses the challenge by reviewing IAM roles, groups, users and policies and providing a report of “least used” IAM roles based on their timestamps. With all the relevant information from ThreatModeler, you can make changes to the access management policies to stay aligned with the LPM. The simulation environment lets CSAs to foresee the effect of policy changes before actually implementing them in AWS accounts.

Q. How does the ThreatModeler integration with AWS SSM help to mitigate possible vulnerabilities?

ThreatModeler assesses the software that is installed on AWS EC2s, identifies the Common Vulnerabilities and Exposures (CVEs) that are tied to it and populates them as threats on the platform.

Q. Will ThreatModeler act on vulnerabilities that are identified from AWS SSM Integration?

A. ThreatModeler shows all the possible CVEs as threats so that CSAs can push these threats as user stories and act on them. This way, the vulnerability cannot be exploited.

Q. Which ThreatModeler editions include these features?

A. ThreatModeler Cloud Edition users can access these features.

Q. How do I get the new release?

A. Please contact your ThreatModeler customer success manager or send an email to support@threatmodeler.com to get the new version.

Q. How can I get help if I have a problem?

ThreatModeler will provide a dedicated Technical Account Manager to help troubleshoot any issues.

Q. What if I have suggestions about how to make ThreatModeler better?

A. You are always welcome to submit feedback, suggestions or a feature request to support@threatmodeler.com.

Stakeholder FAQs

Q. What are the problems that the customer is facing, and how will this integration help them?

A. Anywhere that manual effort is required for access and vulnerability management puts a drain on time, cost and resources. ThreatModeler's integration introduces automated reviews of IAM users, groups and policies and puts a stop to the drain.

Q. What critical challenges will this integration solve?

A. ThreatModeler helps CSAs to reduce the likelihood of over-privileged and least used policies, and the possibility of a data breach from cyber threats.

Q. Who is eligible to access these features?

A. All the customers of ThreatModeler AWS ProServe engagement can take advantage of these features.