ACCELERATING YOUR CLOUD JOURNEY WITH SECURITY BUILT IN

Oct 8, 2020 | Attack Surface Analysis, AWS, CISO, Cloud security, security controls

The move to cloud poses unique challenges as organizations adapt to securing infrastructure as code for all applications, while being prepared to secure brave new features such as containers, microservices and automatic scaling. Threat modeling, traditionally a manual process, would take weeks to enumerate potential threats with diagramming tools or whiteboarding to gain an understanding of your attack surface.

"As we've all learned throughout the years, good compliance doesn't always equal good security, but good security usually means easy compliance."

Tom Holodnik, Intuit

At a high level, DevOps journeying to the AWS cloud involves applying the AWS shared responsibility model, then implementing suitable structures with extremely strict policies to protect customers, data, and workloads in the cloud. Cloud customers are responsible for protecting their workloads while they're in the cloud.

We are moving fast into a world of containerized and serverless workloads, so cloud development processes must change. Part of that AWS cloud adoption framework involves six main focus areas. And one of the main focus areas is security. From that perspective, AWS customers want to take an agile approach to develop security capabilities.

Deploying all your infrastructure as code with security built in is another challenge. Teams must consistently conform to established standards operating in the AWS environment and enforce these standards through processes such as automated checking and automated compliance testing.

Threat modeling enables teams to build a product backlog for moving to the cloud with secure infrastructure, all as code (IaC). IaC becomes your software development functions. While we're all used to doing it in the AppSec world, now we have to get used to it in the infrastructure security world. To achieve this, and meet security and regulatory compliance requirements, DevOps must build Infrastructure security from the ground up.

Accelerate Your Cloud Journey Through Automation

Using ThreatModeler's extensive knowledge base, we can build the learnings, recommended best practices and design patterns needed to accelerate your cloud journey.

Cloud architects and developers will have clear specifications for service configurations and write secure code modules. ThreatModeler has entered a joint offering with AWS that integrates with AWS Security Hub and other native security services. Companies can measure the drift between what is deployed in production versus ideal state threat model blueprints. As teams release new applications and changes to infrastructure, the threat model evolves, surfacing new threats requiring remediation.

ThreatModeler drives the accurate, consistent, repeatable delivery of security requirements, accelerating cloud delivery overall and getting AWS customers to a better place for building out security capabilities themselves.

Learn how to build a threat model with ThreatModeler's one click functionality

Minimize Risk and Go to Market Faster

We are familiar with AWS Service Catalog to build product portfolios. All involved business units need to inherit security vetted code modules. An automated threat modeling program ensures initial modules are secure. From an executive POV, gaining full visibility of your security posture across workloads – from a compliance perspective – will enable you to estimate where to invest your time and resources.

Overall, automated threat modeling will reduce costs, provide a clear picture of your security posture, reduce decision making time, and get security into the hands of developers.

Automate, Integrate, Collaborate

As stated earlier, the ThreatModeler and AWS joint offering leverages AWS security services to handle the complexities of threat modeling to secure cloud applications and infrastructure. AWS customers can now proactively secure their cloud infrastructure using AWS's Security Epics guidance within their threat modeling process, driving security throughout the Cloud Development Life Cycle (CDLC).

Enumerating potential threats with traditional diagramming tools or whiteboarding does not necessarily translate to consistent actionable outcomes. This program automates the process and inserts its outcomes into the CI/CD toolchain. Integration with lifecycle management tools like Jira better position developers to meet tight deadlines. Constant validation occurs by integration with native AWS services such as Security Hub, Config and IAM.

The integrations enable teams to conform with standards. AWS Config yields data insights about your AWS cloud services and AWS Security Hub gets updated on your overall compliance status, providing full visibility of your AWS account in ThreatModeler.

Convert Your Architecture Diagram Into A Threat Model Automatically

ThreatModeler's patent pending Accelerator facilitates a self-service model to automatically generate threat models with threats and security requirements for AWS VPCs at scale.

Post-deployment you can connect with the Accelerator to validate your cloud architecture and the architecture's security automatically. Based on the Read-Only access that ThreatModeler has in the account, ThreatModeler validates that prescribed security requirements have been implemented in your cloud environment.

Teams can assess the drift between what is actually deployed in production against the threat model pattern. Not only keep track of changes to the environment of which you may not be aware, but also evaluate the impact on risk that an application or infrastructure change may cause.

Self-Service Threat Modeling Practice

Implementing a self-service threat modeling practice where all of DevOps can get involved – including developers and CISOs – requires automation, integration and collaboration. Developers can take ownership of threat modeling and security architects become more involved, beyond providing governance and guidance. Security requirements are communicated broadly and DevOps can completely understand the downstream-upstream impact of mitigating application and infrastructure threats.

Working with ThreatModeler helps to continuously mature customers as they are moving to the cloud and ensure continuous security.

Click here to schedule a live demo with a threat modeling expert.

Search

Tags

2020 cybersecurity Amazon Application Security application threat model application threat modeling attack surface analysis AWS AWS Security Epics Automated AWS Threat Modeling Blog CDLC Channel Futures CISO cloud computing cloud development life cycle Cloud Security collateral damage cybercrime cybersecurity Dark Reading data breach data breaches Data Security DevOps DevSecOps Dice Forbes internet of things IoT IoT Security one-click threat modeling Press Release proactive security ransomware Risk Management SC Magazine Security Boulevard security by design Security Magazine Tech News World ThreatModeler Threat Modeling Threat Post VM Blog ZDNet

Latest Posts


Why Threat Modeling?


Can You Code Your Way to Cybersecurity?


One Good Way to Know if Developers are Developing Secure Code

Agile Development: What You Need to Know


Understanding Live Cloud Environment and Threat Modeling