EINPRESSWIRE

RAD Security Launches First AI-Powered Incident Investigation with Behavioral Detection & Response Platform

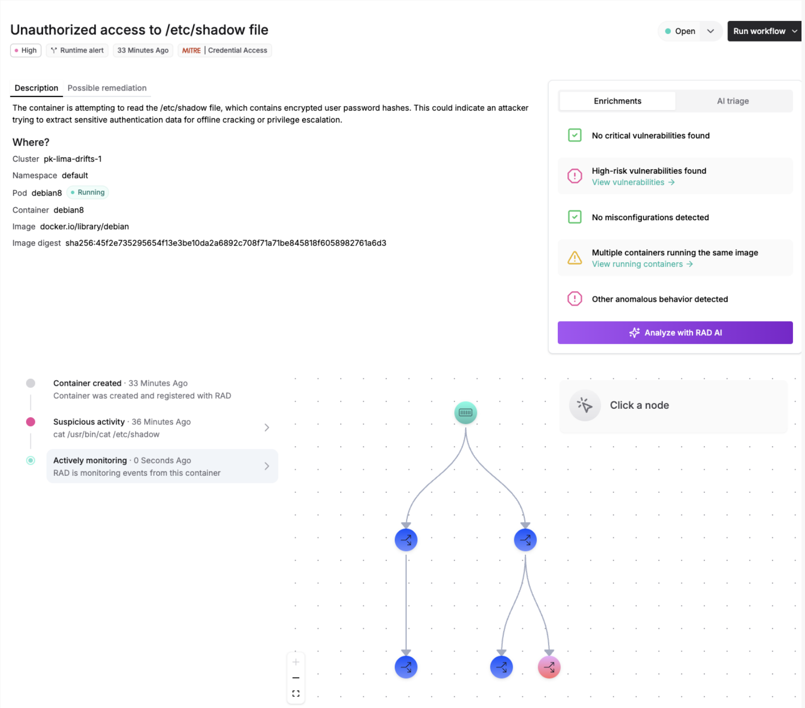
AI-powered investigation combined with behavioral detection and response reduces false positives for time-strapped detection engineers

SAN FRANCISCO, CA, UNITED STATES, August 6, 2024 /EINPresswire.com/ -- Today, as RAD Security takes the stage as a finalist in the Black Hat Startup Spotlight Competition, it unveils the first-ever AI-powered incident investigation capability for behavioral detection and response. Today, cloud security is based almost exclusively on signature-based detections, which are notorious for burdening security teams with false positives. RAD Security is the first to combine AI-powered incident investigation with behavioral, signature-less detections, to significantly reduce false positives and provide much-needed relief for overburdened security teams.

> “
> By adding AI-powered investigations to behavioral detection, security teams can quickly get light years ahead in the accurate assessment of incidents.”
> *Jimmy Mesta, CTO and Co-Founder*

“By definition, signatures are stateless, making investigations based on the signature-focused approach inaccurate and tedious,” says CTO and Co-Founder Jimmy Mesta. “By adding AI-powered investigations to behavioral detection, which is already a step ahead of signature-based detection in accuracy, security teams can quickly get light years ahead in the accurate assessment of incidents.”

RAD’s behavioral approach and AI-powered investigations result in the lowering of false positives on their own; but by putting these two capabilities together, RAD enables security teams to achieve a multiplier effect. The enhanced accuracy of behavioral methods versus signature-based methods is easily demonstrated using multiple examples of attack tactics like reverse shells, access to sensitive data, and a Sudo CVE. In these examples, while signatures can be easily bypassed by avoiding the exact parameters, they are detected by RAD’s behavioral solution. By the same token, a behavioral drift event is not always a malicious event, so the addition of the AI investigation capability ensures additional accuracy. AI is particularly suited for looking across large sets of data and quick contextualization, making it a natural investigation tool and engine to analyze benign versus malicious drift.



Unauthorized access to /etc/shadow file

The container is attempting to read the /etc/shadow file, which contains encrypted user password hashes. This could indicate an attacker trying to extract sensitive authentication data for offline cracking or privilege escalation.

Where?

Cluster pk-lima-drifts-1
Namespace default
Pod debian8 Running
Container debian8
Image docker.io/library/debian
Image digest sha256:45f2e735295654f13e3be10da2a6892c708f71a71be845818f6058982761a6d3

No critical vulnerabilities found
High-risk vulnerabilities found
No misconfigurations detected
Multiple containers running the same image
Other anomalous behavior detected

Container created · 33 Minutes Ago
Container was created and registered with RAD

Suspicious activity · 36 Minutes Ago
cat /usr/bin/cat /etc/shadow

Actively monitoring · 0 Seconds Ago
RAD is monitoring events from this container

Screenshot of AI capabilities from RAD

Throughout the history of cyber security, and most famously in the endpoint and network security markets, signatures have eventually been replaced by behavioral methods in response to an evolving threat landscape. Today, the cloud security category is nearly entirely composed of signature-based approaches with runtime security and Cloud Workload Protection (CWPP) that are standalone or part of a broader Cloud Native Application Protection Platform (CNAPP). In sharp contrast to signature-based CNAPPs, or posture-focused Cloud Security Posture Management (CSPM), RAD Security's Cloud Detection and Response (CDR) solution creates behavioral baselines of unique good behavior to detect zero day attacks, enriching detections with real-time identity and infrastructure context that inform response actions.

More and more, detection and response is being accomplished by fewer and fewer dedicated people, with 22% of security professionals reporting recent layoffs at their company. The workforce reductions are an even more acute pain in cloud security, with 65% of cybersecurity and infosecurity professionals claiming burnout due to skill gaps. Even though a full 95% of IT decision makers feel their team has been negatively impacted by the cloud security skills gap, cloud native adoption continues, and analysts predict that, by 2025, 95% of new applications will be built using cloud native workloads.

Zero days like the XZ Backdoor are now a regular occurrence, making detection and response in cloud native environments more important than ever.

RAD Security has introduced multiple new features to help security teams adopt new innovation that will help them address these alarming trends and emerging threats:
- Amazon EKS Add-on: RAD Security is now available as an Amazon EKS Add-on in the AWS Marketplace for Containers. This means customers can now provision the real-time KSPM and runtime features of the RAD platform directly from EKS, for real-time visibility into their Kubernetes risk as well as signatureless cloud detection and response.

- Automated AI-Powered Investigation: RAD Security uses LLMs to quickly analyze multiple behavioral detections and determine whether an incident is malicious or benign, including real-time infrastructure and identity context.
- Findings Center: All incidents are now available in an easy to navigate console, making detection and investigation easier and quicker.
- RAD Open Source Catalog: New version details and new open source images have now been added to the RAD Catalog, detailing the changes in behavioral fingerprints over time and bolstering the behavioral workload fingerprint standard.

Schedule a meeting with the RAD Security team at the Black Hat Conference this week to discuss improving detection accuracy for attacks in your cloud environments. The team will be exhibiting at booth #219 in Startup City, and at 4:45PM EST they will be presenting at the Innovators and Investors Summit as one of the four finalists in the Startup Spotlight competition.

About RAD Security (formerly KSOC)
RAD Security is a cloud native security company that empowers engineering and security teams to push boundaries, build technology and drive innovation so they can focus on growth versus security problems. In sharp contrast to signature-based, one-size-fits-all, legacy CWPP and container security solutions, RAD takes a signature-less, behavioral approach to detect and respond earlier to cloud attacks while sharpening inputs into shift-left and posture management.

Daniel Delson
Magnitude Growth
+1 917-328-9337
email us here
Visit us on social media:
X
LinkedIn
YouTube