THE ANATOMY OF A **THREAT STACK**
INSIGHT REPORT

The Threat Stack Cloud SecOps Program℠ includes two services to help you get the most from your Threat Stack experience: Threat Stack Oversight℠, and Threat Stack Insight℠. Insight turns our Security Operations Center (SOC) into a team of cloud-security consultants for your business. With Insight, we monitor your environment and deliver custom analytics each month to help you identify and remediate vulnerabilities in your cloud infrastructure.

HERE'S HOW IT WORKS

1. Each month, your analyst pulls data for 5 KPIs from your cloud environment
2. Your analyst reviews the data—looking for vulnerabilities in your infrastructure
3. The analyst creates a quarterly report to help you proactively reduce risk

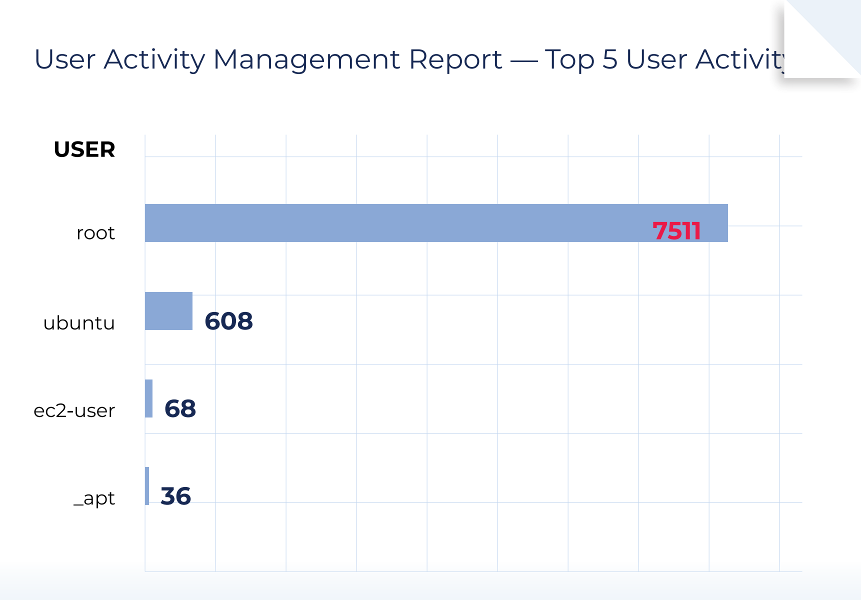
INSIDE AN INSIGHT REPORT

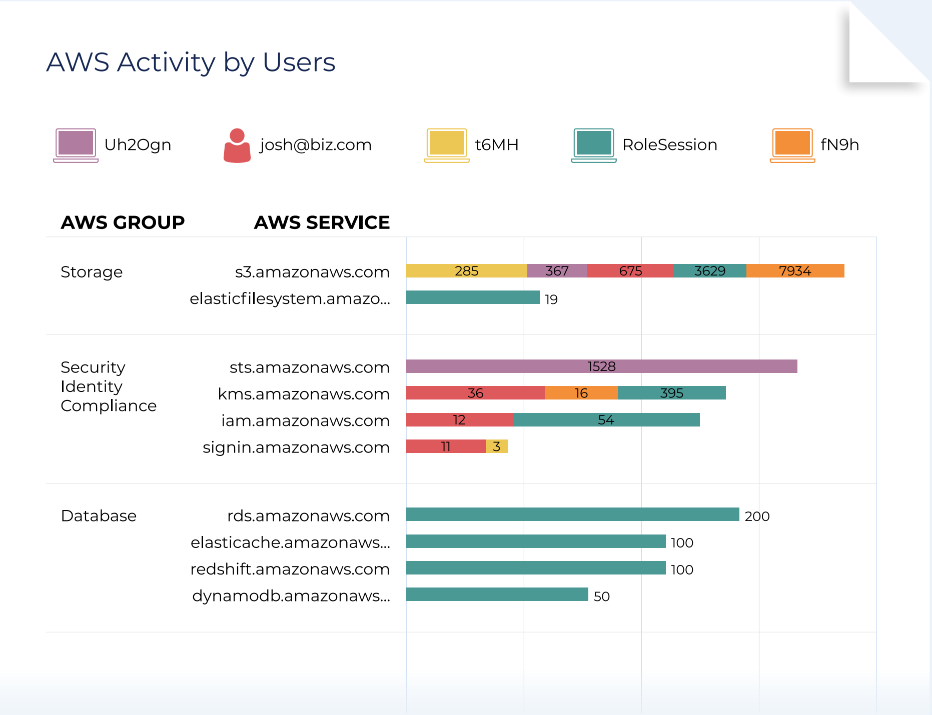
USER: ROOT

What We Observed
Root user is over-utilized.

Why It's Risky
Depending on the type and frequency of the activity, this behavior could be associated with automated activity.

Steps To Remediate
Give users and services appropriate permissions so they don't need to rely on root. For example, Kubernetes-related services do not require root privileges, so scoped users can be created in order to conduct these types of activities.





CLOUDTRAIL: AWS Activity by User

What We Observed
The RoleSession user is accessing the RDS service, which may contain customer data.

Why It's Risky
Low visibility into which users are accessing specific AWS services leaves your infrastructure vulnerable—this could represent excessive permissions.

Steps To Remediate
Follow the principle of least privilege. Only give users the access they need, and track all instances of privilege escalation within AWS.

VULNERABILITIES

What We Observed
Unpatched servers are resulting in high-severity vulnerabilities.

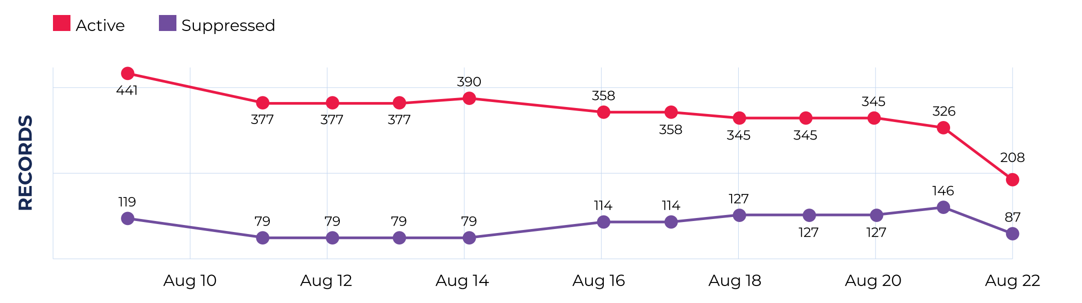
Why It's Risky
The more vulnerabilities a server has, the more likely they will be exploited, especially if the server is internet-facing.

Steps To Remediate
Standardize and automate your patching process.

Active Vulnerabilities

SEVERITY	IMAGE ID	CVE	CVSS SCORE
HIGH	ami-6057e21a	CVE-2015-2806	10.000
		CVE-2017-16844	10.000
		CVE-2015-2328	7.500
		CVE-2016-3191	7.500
	ami-c58c1dd3	CVE-2015-2806	10.000
		CVE-2017-16844	10.000
		CVE-2015-2328	7.500
		CVE-2016-3191	7.500

Trending CVEs



INSIGHTS THAT MAKE A DIFFERENCE

With custom Insight reports, you can develop a proactive strategy with automation and long-term security in mind. Now you can focus on growing your business while bridging the gap between your Security and Operations teams.

5 Key Metrics

Insight reports analyze every aspect of your infrastructure to help you reach SecOps Maturity, including:

- Network Activity
- AWS Security
- File Behavior Management
- User Activity Management
- Vulnerability Assessment

In-Depth Reports. Expert Review.

Each month, you can review your Insight report with a Cloud SecOps coach. Your coach will help you set security goals and track your progress. It's like having a personal trainer for your cloud security.

younique

"We're able to see what instances have the greatest need for assessment and remediation and we move down the list on those. Over time, that's going to substantially improve our overall security structure."

Vincent Romney
Director of InfoSec, Younique

Make the Threat Stack Security Operations Center part of your team.
Learn more at threatstack.com/insight

threat stack

Source: Threat Stack