Observation and Analysis: Our Insights Service

Ongoing Analysis from Our Experts to Improve Your Security Posture Over the Long Term

Securing your public cloud environment requires a fundamentally different approach compared to securing legacy infrastructure—but it's challenging to know where to start or how to move from reactive risk management to a more proactive stance.

The F5® Distributed Cloud App Infrastructure Protection (AIP), formerly known as Threat Stack, Insights service helps you build a Cloud SecOps strategy based on your actual infrastructure risk. Unlike consulting services or frameworks that give you a list of technology to implement, Distributed Cloud AIP Insights hinges on data and analytics that are pulled from the Distributed Cloud AIP solution and are curated for you by our expert security analysts. As part of the service, you receive written recommendations and strategy coaching sessions, so you can prioritize and set goals for improving your overall security posture.

What You Get

- Trend, detection-in-depth, vulnerability, and anomaly reporting
- Recommendations to reduce risky behavior
- Cloud SecOps strategy sessions and ongoing coaching

How It Works

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

Key Metrics

Distributed Cloud AIP Insights reports analyze every aspect of your infrastructure to help you reach SecOps maturity, including:

- Network Activity

- AWS Security

- File Behavior and User Activity Management

- Vulnerability Assessment

Here are a few samples of the kinds of insights you might receive, taken from a portion of a sample Distributed Cloud AIP Insights report:
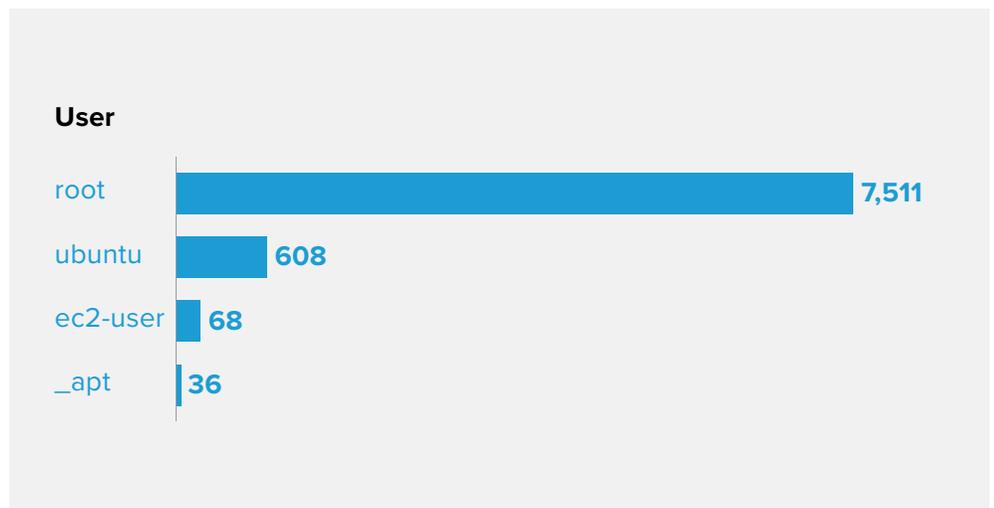
User

root	7,511
ubuntu	608
ec2-user	68
_apt	36

Figure 1: User: Root—User Activity Management Report—Top 4 User Activities

What We Observed

Root user is over-utilized.

Why It's Risky

Depending on the type and frequency of 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 privileges, so scoped users can be created in order to conduct these types of activities.

AWS Group	AWS Service	t6MH	Uh2Ogn	josh@biz.com	Role Session	fN9h
Storage	s3.amazonaws.com	285	367	675	3,629	7,934
	elasticfilesystem.ama…				19	
Security Identity Compliance	sta.amazonaws.com		1,528			
	kms.amazonaws.com			36	395	16
	iam.amazonaws.com			12	54	
	signin.amazonaws.com	3		11		
Database	rds.amazonaws.com				200	
	elasticache.amazona…				100	
	redshift.amazonaws.c…				100	
	dynamab.amazonaws…				50	

Figure 2: CloudTrail: AWS Activity by Users

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 with AWS.
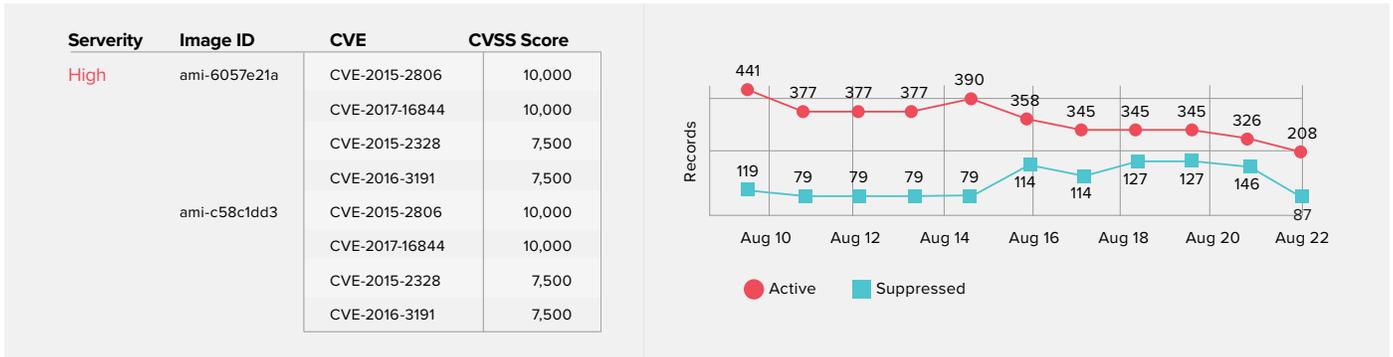
Serverity	Image ID	CVE	CVSS Score
High	ami-6057e21a	CVE-2015-2806	10,000
		CVE-2017-16844	10,000
		CVE-2015-2328	7,500
		CVE-2016-3191	7,500
	ami-c58c1dd3	CVE-2015-2806	10,000
		CVE-2017-16844	10,000
		CVE-2015-2328	7,500
		CVE-2016-3191	7,500

Figure 3: Active Vulnerabilities and Trending CVEs

What We Observed

Unpatched servers are resulting in high-severity vulnerabilities.

Why It's Risky

The more vulnerabilities a servers has, the more likely they will be exploited, especially if the server is internet-facing.

Steps to Remediate

Standardize and automate your patching process.

Threat Stack: Now Part of F5

Threat Stack is now F5 Distributed Cloud App Infrastructure Protection (AIP). If you'd like to learn more about this solution, the company's Security Operations Center (including Distributed Cloud AIP Managed Security Services and Distributed Cloud AIP Insights), and more, feel free to contact our cloud security and compliance experts.

Let our experts take your cloud security worries off your shoulders, so you can get down to business. To learn more or to schedule a demo, visit our website today.