Positka

CloudSecMon

POSITKA'S Cloud Security Monitoring Solution

Analytics-Driven and Real Time Security Monitoring for Modern Threats

With the increased adoption of hybrid cloud, multi cloud and SaaS services, the threat surface for organizations has expanded exponentially

The heightened risks associated with data breach, data exposure and account compromise in the cloud context require robust monitoring solutions to be in place

A cloud monitoring solution should be able to detect threats in real time, as well as provide historical views for forensics, threat hunting and for potential compliance / regulatory needs

Cloud Security monitoring is used to monitor, analyse, detect and neutralize threats across your Cloud infrastructer and applications

Lacking a central monitoring and response solution, it is difficult for organizations (and security teams) to have oversight of an increasingly complex and ever changing cloud environment

ORGANIZATIONS NEED TO CONSIDER SECURITY FOR PUBLIC CLOUD

CHALLENGES

- Operate in complex Hybrid & Multi cloud environments
- Work with multiple services & data sources monitoring
- Tackle growing instances of security breaches
- Overcome challenges linked with multi cloud startegy
- Monitor for unauthorized data access
- Reduce chance of data loss
- Get control over insecure APIs / API calls
- Address low SOC visibility over Cloud platforms

DESIRED BENEFITS / OUTCOMES

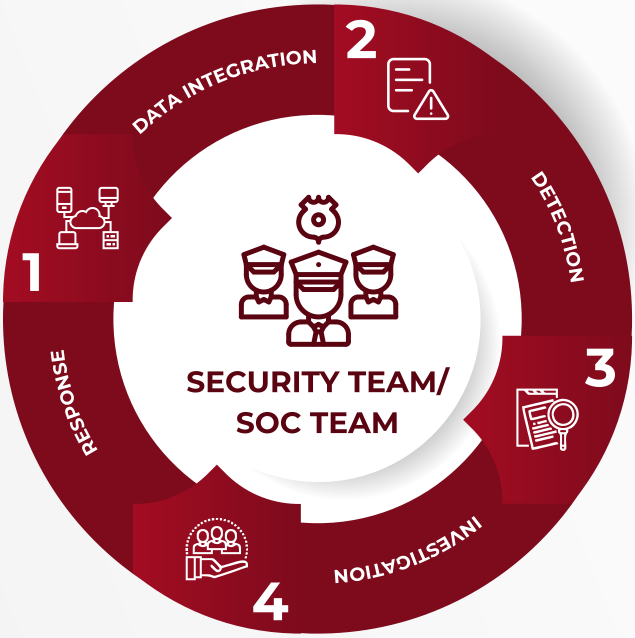
- Some of the key benefits to be obtained from Positka's Cloud Security Monitoring solution are:
- Enhanced security posture and reduce risk
- Increase speed of response to threats
- Improve ROI by increasing efficiency
- Provide independent oversight of cloud
- monitoring to security teams
- Adopt a future ready solution with changing requirements

CONTACT US

✉ susan@postika.com

www.positka.com

DESIGNING AN EFFECTIVE CLOUD SECURITY MONITORING SOLUTION

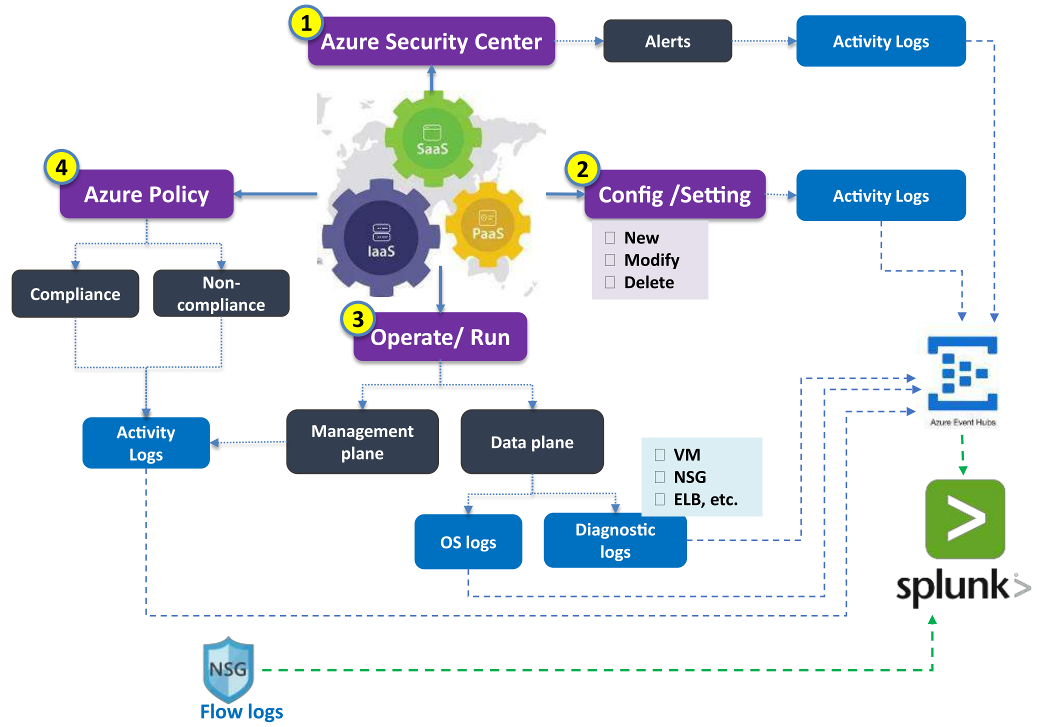


Positka's Cloud Security Monitoring Solution helps security teams streamline security operations for organizations of all sizes and levels of expertise.

- ☆ **Insight from data** that is automatically retrieved from cloud services, and data sources [Log/API]
- ☆ **Correlation rules** which generate alerts for the rapid detection and analysis of advanced threats. Achieve increased levels of operational visibility without additional complexity.
- ☆ **Flexibility to customize** dashboards, reports, correlation searches as required- deployed for continuous monitoring incident responses who needs to view the risks taking place in the cloud
- ☆ **Analytics driven security -** The process of discovering relationships across all the security relevant data to a changing threat landscape

DATA INTEGRATION ILLUSTRATION: DATA SOURCES FOR AZURE

The Azure Platform services provide data routing and access for Azure resources. Azure exposes three main types of data like Metrics, Diagnostic logs and Activity logs. Components like AD Application, Event Hub are involved in the data source collection which can be seen in the illustrative picture below.

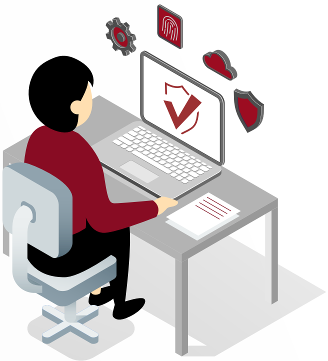


1. SINGLE PANE OF GLASS VISIBILITY

aws

Azure

Google Cloud



NETWORK

STORAGE

COMPUTE

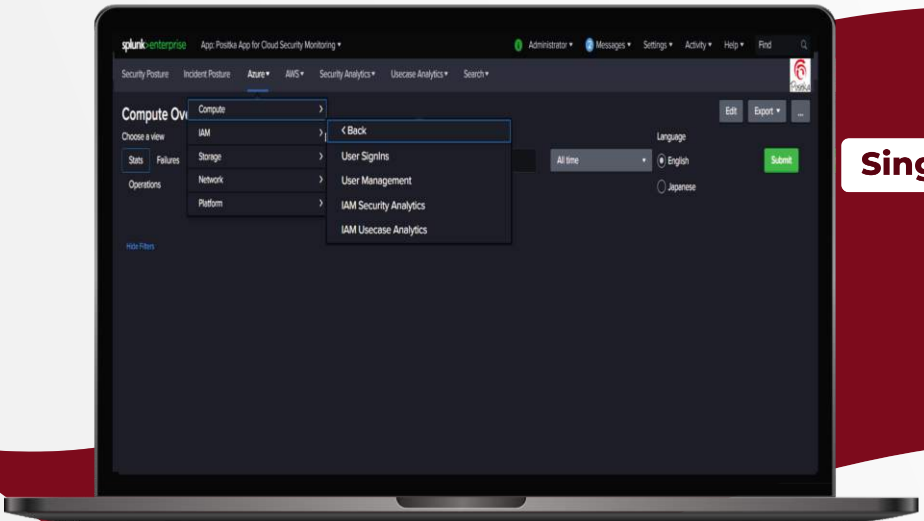
IAM

Positka's Cloud Security Monitoring solution for cloud services provides an effortless experience in configuring and monitoring all cloud platform logs from AWS, Azure and GCP across services like Network, Compute, Storage and IAM.

Benefits include:

- ☆ Gathering of important insights into security-related activities such as unauthorized access attempts, network configuration changes.
- ☆ Increased visibility into user behaviour and resource utilization.
- ☆ Audit trail logging improves adherence to security and compliance requirements.

Using **Positka's Cloud Security Monitoring solution** makes it easier to visualize and consume data for developers, system administrators and security professionals under one easy to manage interface.



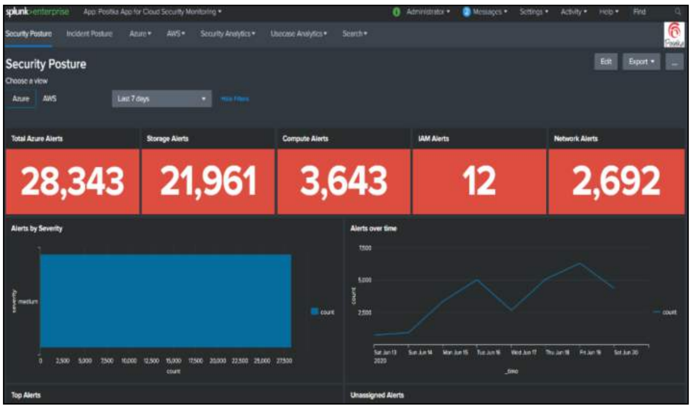
Single Pane Of Complete Insights

Positka's Cloud Security Monitoring Solution provides a **single pane of glass** view to bring an Analytics driven perspective to cloud monitoring.

2. SECURITY POSTURE DASHBOARD

The Security Posture Dashboard gives a consolidated view of key metrics, making it easier for the organization to make key decisions.

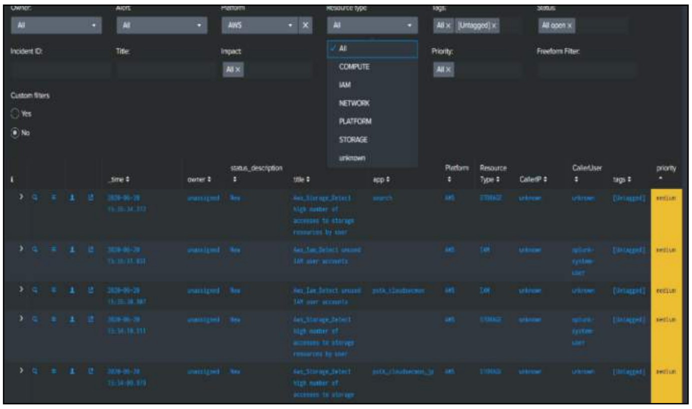
This security posture helps to understand what has happened across the cloud environment and helps determine if a cloud resource might have been compromised.



Security Posture

Total Azure Alerts	Storage Alerts	Compute Alerts	IAM Alerts	Network Alerts
28,343	21,961	3,643	12	2,692

3. INCIDENT RESPONSE WORKFLOW



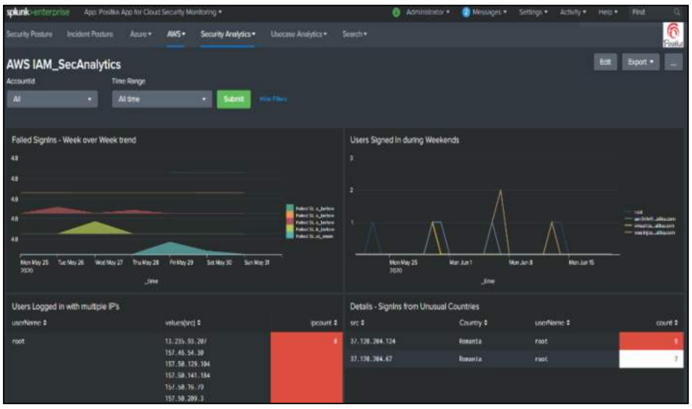
i					_time ⇕	owner ⇕	status_description ⇕	title ⇕	app ⇕	Platform ⇕	Resource Type ⇕	CallerIP ⇕	CallerUser ⇕	tags ⇕	priority ^
›					2020-06-20 [illegible]	unassigned	New	Aws_Storage_Detect high number of accesses to storage resources by user	search	AWS	STORAGE	unknown	unknown	[Untagged]	medium
›					2020-06-20 [illegible]	unassigned	New	Aws_Iam_Detect unused IAM user accounts		AWS	IAM	unknown	splunk-system-user	[Untagged]	medium
›					2020-06-20 [illegible]	unassigned	New	Aws_Iam_Detect unused IAM user accounts	posh_cloudsecmon	AWS	IAM	unknown	unknown	[Untagged]	medium
›					2020-06-20 [illegible]	unassigned	New	Aws_Storage_Detect high number of accesses to storage resources by user		AWS	STORAGE	unknown	splunk-system-user	[Untagged]	medium
›					2020-06-20 [illegible]	unassigned	New	Aws_Storage_Detect high number of accesses to storage	posh_cloudsecmon_[illegible]	AWS	STORAGE	unknown	unknown	[Untagged]	medium

Optimize incident response workflows by utilizing the intergrated incident response workflow.

Assign and track alerts from inception to remediation and closure.

4. SECURITY ANALYTICS VIEW

The Security Analytics view helps conduct rapid investigations using ad hoc searches , as well as static, dynamic and visual correlations to investigate threats or attacks happening in the cloud environment. Get insights with actionable information to reduce risk, threat context and track attacker steps to verify evindence



AWS IAM_SecAnalytics

Users Logged in with multiple IP's

userName ⇕	values(src) ⇕	ipcount ⇕
root	13.235.93.207 157.46.54.30 157.50.129.104 157.50.141.184 157.50.16.79 157.50.209.3	6

Details - SignIns from Unusual Countries

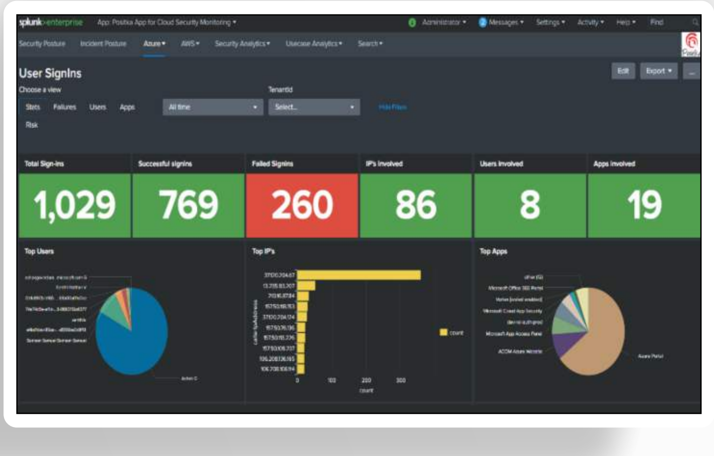
src ⇕	Country ⇕	userName ⇕	count ⇕
37.120.204.124	Romania	root	1
37.120.204.67	Romania	root	2

CONTACT US

susan@postika.com

www.positka.com

5. SERVICE OVERVIEW ACTIVITY PANE



splunk>enterprise App: Positka App for Cloud Security Monitoring

Security Posture | Incident Posture | Azure | AWS | Security Analytics | Usecase Analytics | Search

User SignIns

Choose a view: Stats, Failures, Users, Apps, Risk

All time

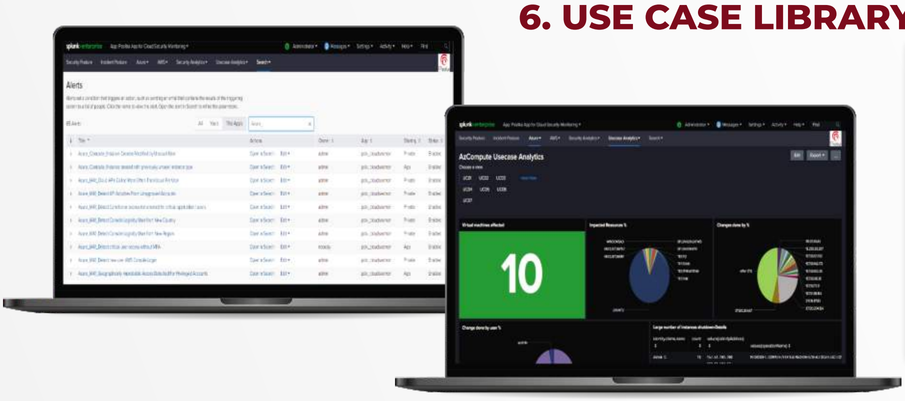
TenantId: Select...

Total Sign-ins	Successful signins	Failed SignIns	IP's involved	Users involved	Apps involved
1,029	769	260	86	8	19

The Security Overview dashboards provide detailed information about the activity happening within specific service in your cloud environment.

It also contains multiple filters to help drill down into specific resources to be invetigated.

6. USE CASE LIBRARY/ALERTS



A sophisticated library of use cases across services helps drive the real-time monitoring for threats. Use cases comprise of alerts (rules) and corresponding dashboards, which help security analysts to quickly investigate potential incidents.

SOME ILLUSTRATIVE USE CASES

IAM

- Detect critical user access without MFA.
- High privilage user deleted.
- Detecting login from multiple IP/device by user.

STORAGE

- Detect storage accessed by anomalous user/location.
- Detect disabling of protection for critical resources.
- Detect high number of storage create/ delete.

COMPUTE

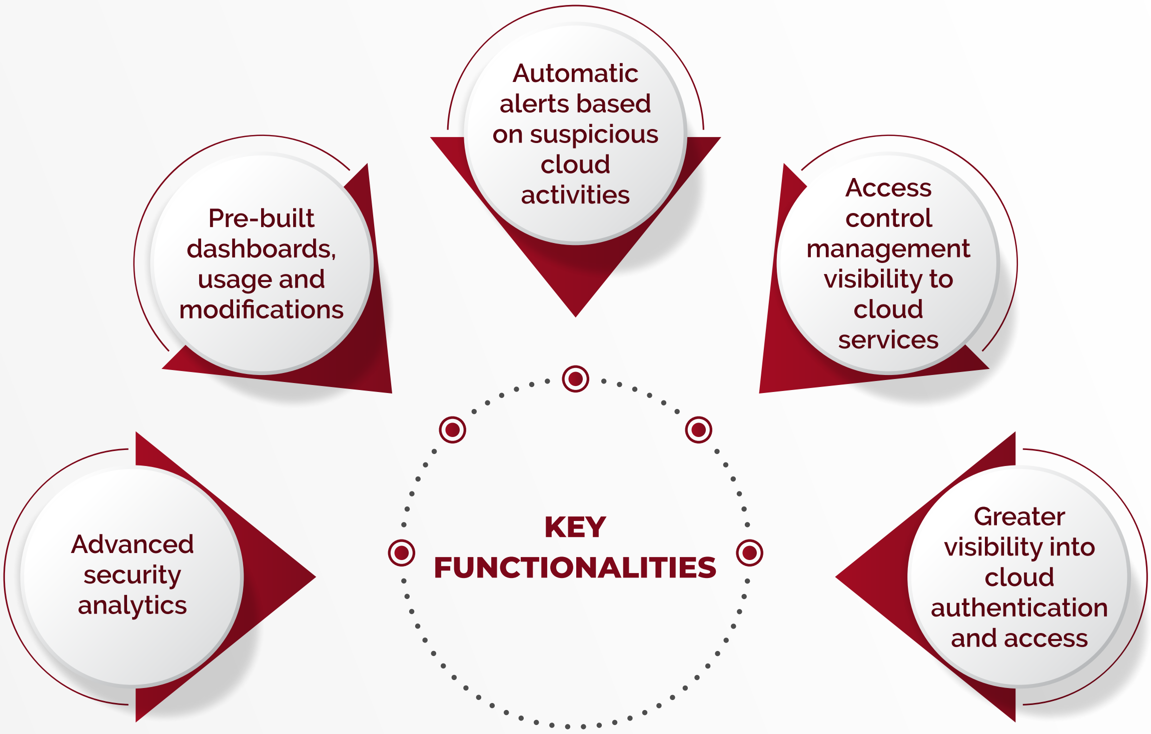
- Detect instance modification by unusual user.
- Monitor for role/ permission changes for instance.
- Monitor for Unusual instance shut down critical resources.

NETWORK

- Detect unusual Number of Modifications to cloud ACLs.
- Monitor for Network Access Control List Created with All Open Ports.
- Modification of network ACL from unuasual location.

WHY POSITKA'S CLOUD MONITORING SECURITY SOLUTION

- Visibility can also be a concern when it comes to cloud monitoring.
- Many companies rely on third-party cloud services providers and may not have access to every layer in the cloud computing stack, and therefore cannot gain full visibility to monitor for potential security flaws and vulnerabilities.
- One of the most effective ways to mitigate cloud security risks is to gain complete control over data from all sources to gain a comprehensive view of the entire environment



KEY FUNCTIONALITIES

Automatic alerts based on suspicious cloud activities

Pre-built dashboards, usage and modifications

Access control management visibility to cloud services

Advanced security analytics

Greater visibility into cloud authentication and access

INSTALLATION NOTES:

The monitoring solution is deployed on the Splunk Enterprise platform. An existing Splunk Enterprise installation with a valid license is a prerequisite for installing the monitoring solution.

Use cases are currently available for the following Public Cloud services on Azure and AWS-Compute, Storage, IAM, Network, Platform.