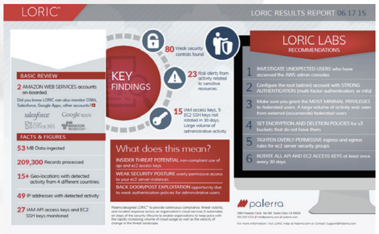
SOLUTION BRIEF

LORIC™ for amazon web services™



LORIC™ LORIC RESULTS REPORT 06.17.15

BASIC REVIEW

2 AMAZON WEB SERVICES accounts on-boarded.

Did you know LORIC can also monitor O365, Salesforce, Google Apps, other accounts?

FACTS & FIGURES

53 MB Data ingested

209,300 Records processed

15+ Geo-locations with detected activity from 4 different countries

49 IP addresses with detected activity

27 IAM API access keys and EC2 SSH keys monitored

KEY FINDINGS

80 Weak security controls found

23 Risk alerts from activity related to sensitive resources

15 IAM access keys, 5 EC2 SSH keys not rotated in 30 days. Large volume of administrative activity

What does this mean?

INSIDER THREAT POTENTIAL non-compliant use of api and ec2 access keys

WEAK SECURITY POSTURE overly-permissive access to your ec2 server instances

BACK DOOR/POST EXPLOITATION opportunity due to weak authentication policies for administrative users

Palerra designed LORIC™ to provide continuous compliance, threat visibility, and incident response across an organization's cloud services. It automates all steps of the security lifecycle to enable organizations to keep pace with the rapidly increasing volume of cloud usage as well as the velocity of change in the threat landscape.

LORIC LABS
RECOMMENDATIONS

1 INVESTIGATE UNEXPECTED USERS who have accessed the AWS admin consoles

2 Configure the root (admin) account with STRONG AUTHENTICATION (multi-factor authentication, or mfa)

3 Make sure you grant the MOST MINIMAL PRIVILEGES to federated users. A large volume of activity was seen from external (assumerole) federated users

4 SET ENCRYPTION AND DELETION POLICIES for s3 buckets that do not have them

5 TIGHTEN OVERLY-PERMISSIVE ingress and egress rules for ec2 server security groups

6 ROTATE ALL API AND EC2 ACCESS KEYS at least once every 30 days

palerra
3945 Freedom Circle Ste 560 Santa Clara CA 95054
650 300 5222 /// info@palerra.com /// palerra.com

For more information: Visit LORIC Help at Palerra.com or Contact Support@Palerra.com

Get a free assessment of usage, threats and compliance violations in your AWS environment

Cloud Security is a Shared Responsibility

Cloud services are a growing target and in extreme cases, breaches have put companies out of business. Code Spaces is one such example where it had to close doors in June 2014 after hackers gained privileged access to its Amazon Web Services (AWS) environment and destroyed critical assets.

Protection of workloads and data is a priority for Amazon and it takes numerous steps to reduce risk. However, cloud security is a shared responsibility between the organization and the cloud provider.

AWS Shared Responsibility Model

Source: http://aws.amazon.com/compliance/shared-responsibility-model/

> *"While AWS manages security of the cloud, security in the cloud is the responsibility of the customer. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would for applications in an on-site datacenter."*

An organization's obligations include being able to answer questions such as:

- Are privileged users creating new admin accounts that may potentially create backdoors to the environment?
- Are any privileged users spinning up or terminating instances without approval?
- Is there risk from users that have not rotated access key pairs?

There are a number of challenges in meeting these obligations:

- Detection of anomalous activity is challenging due to the volume of log data, lack of activity baselines, and lack of context
- Manual monitoring of security configurations and activities is laborious and error-prone
- Remediation requires subject matter expertise in AWS

Security & Governance for AWS

Palerra enables organizations to protect data within AWS with LORIC™, the cloud security automation platform. It is the only solution to manage the entire security lifecycle of cloud infrastructure in a single platform.

VISIBILITY: Insights into AWS usage

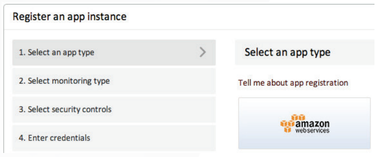
THREAT DETECTION: Monitoring for anomalous activities

COMPLIANCE MANAGEMENT: Monitoring of configurations and activities leading to policy violations

INCIDENT RESPONSE: Logging and remediation

Automation of threat detection, compliance management and incident response with LORIC increases operational efficiency and enables staff to focus on more strategic initiatives. It is delivered as a service and can be deployed in minutes. LORIC enables security and governance for AWS.

EFFORTLESS DEPLOYMENT



Register an app instance

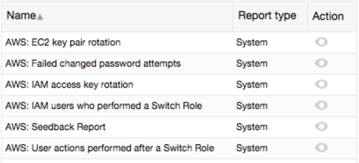
1. Select an app type
2. Select monitoring type
3. Select security controls
4. Enter credentials

Select an app type

Tell me about app registration

Get started in minutes by creating an AWS service account for LORIC. No hardware, no software, no agents.

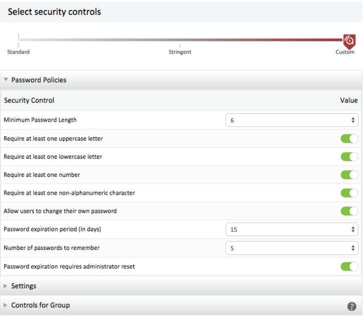
ACTIVITY REPORTS



Name▲	Report type	Action
AWS: EC2 key pair rotation	System	◉
AWS: Failed changed password attempts	System	◉
AWS: IAM access key rotation	System	◉
AWS: IAM users who performed a Switch Role	System	◉
AWS: Seedback Report	System	◉
AWS: User actions performed after a Switch Role	System	◉

Ability to create custom reports as well as a rich set of predefined reports on potentially risky activities such as switching roles.

CONFIGURATION MONITORING



Select security controls

▾ Password Policies

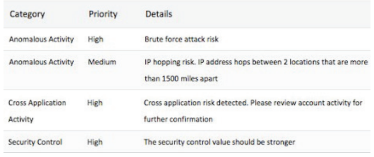
Security Control	Value
Minimum Password Length	6
Require at least one uppercase letter	●
Require at least one lowercase letter	●
Require at least one number	●
Require at least one non-alphanumeric character	●
Allow users to change their own password	●
Password expiration period (in days)	15
Number of passwords to remember	5
Password expiration requires administrator reset	●

▸ Settings

▸ Controls for Group

Continuously monitors and enforces security configurations within AWS to ensure compliance – say goodbye to laborious manual audits.

AUTOMATIC INCIDENT RESPONSE

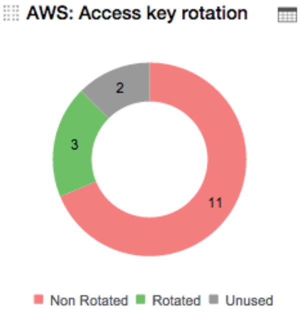


Category	Priority	Details
Anomalous Activity	High	Brute force attack risk
Anomalous Activity	Medium	IP hopping risk. IP address hops between 2 locations that are more than 1500 miles apart
Cross Application Activity	High	Cross application risk detected. Please review account activity for further confirmation
Security Control	High	The security control value should be stronger

Automatically logs incidents and executes remedial actions within AWS ensuring incidents are addressed immediately.

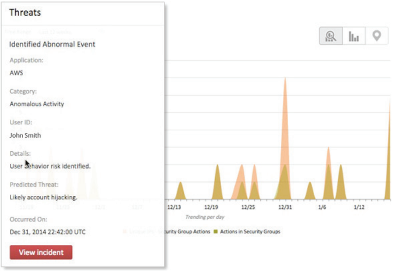
INSIGHTS

Instant insights into adoption and usage of AWS, such as status of access key rotations.



USER BEHAVIOR ANALYTICS

Studies activities such as logins and environment administration to create baseline activity profiles. It then automatically flags any deviations in behavior exposing insiders and hackers.



Threats

Identified Abnormal Event

Application:
AWS

Category:
Anomalous Activity

User ID:
John Smith

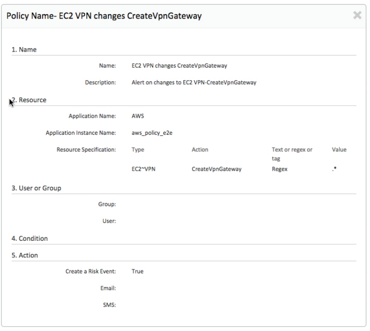
Details:
User behavior risk identified.

Predicted Threat:
Likely account hijacking.

Occurred On:
Dec 31, 2014 22:42:00 UTC

MONITORING POLICIES

Ability to build custom policies as well as a library of predefined policies for real-time notifications about activities that may introduce risks, such as termination of EC2 instances.



Policy Name- EC2 VPN changes CreateVpnGateway

1. Name

Name: EC2 VPN changes CreateVpnGateway

Description: Alert on changes to EC2 VPN-CreateVpnGateway

2. Resource

Application Name: AWS

Application Instance Name: aws_policy_e2e

Resource Specification:

Type	Action	Text or regex or tag	Value
EC2~VPN	CreateVpnGateway	Regex	.*

3. User or Group

Group:

User:

4. Condition

5. Action

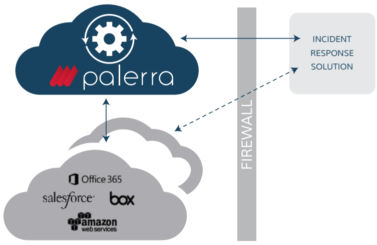
Create a Risk Event: True

Email:

SMS:

ECOSYSTEM INTEGRATION

Leverages existing IT investments by integrating with LDAP, single sign on, identity and access management, ticketing, and incident management solutions.



palerra
INCIDENT RESPONSE SOLUTION
FIREWALL
Office 365
salesforce
box
amazon web services