# About Skyhigh for AWS

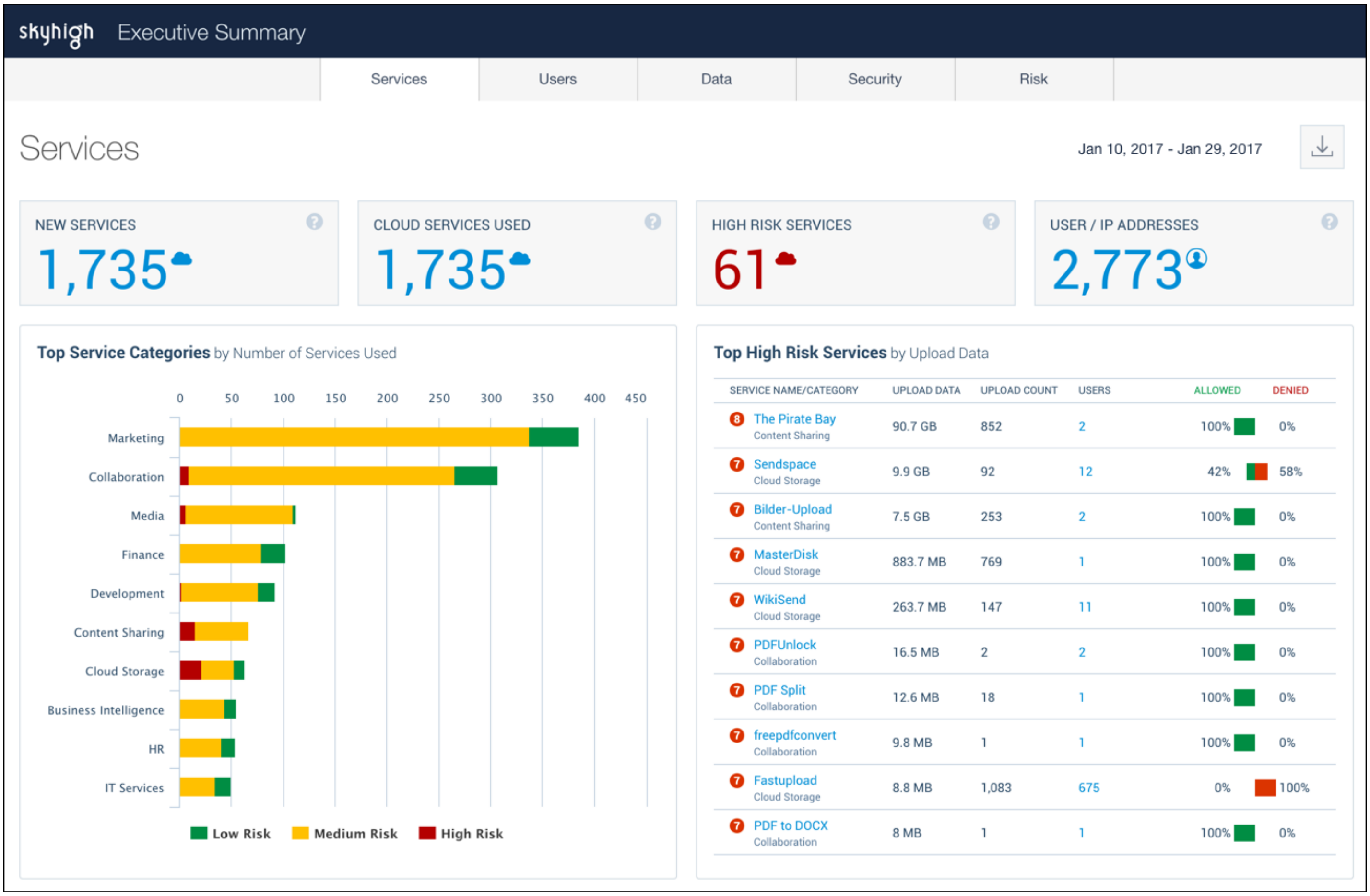
Skyhigh for AWS extends Skyhigh features to monitor, secure, and audit AWS environments for threat protection, anomaly detection, configuration audit, and forensic audit logs. Skyhigh provides this capability by leveraging public AWS APIs.

Skyhigh for AWS has SOC-sepecific threat protection and incident response workflows to remediate potential insider threats, privileged user threats, and compromised accounts.

# CloudTrail Logging

Leveraging AWS CloudTrail, Skyhigh for AWS captures activities to give new insight into activities, and to support post-incident investigations and forensics.

CloudTrail logs are used to profie current cloud application security settings and suggests modifications to improve security based on industry best practices. Skyhigh continuously monitors AWS configuration against regulatory requirements to streamline internal and external audits, such as ISO 27008, PCI, HIPAA, etc.



Services

Jan 10, 2017 - Jan 29, 2017

| NEW SERVICES | CLOUD SERVICES USED | HIGH RISK SERVICES | USER / IP ADDRESSES |
|---|---|---|---|
| 1,735 | 1,735 | 61 | 2,773 |

**Top Service Categories** by Number of Services Used

**Top High Risk Services** by Upload Data

| SERVICE NAME/CATEGORY | UPLOAD DATA | UPLOAD COUNT | USERS | ALLOWED | DENIED |
|---|---|---|---|---|---|
| 8 The Pirate Bay<br>Content Sharing | 90.7 GB | 852 | 2 | 100% | 0% |
| 7 Sendspace<br>Cloud Storage | 9.9 GB | 92 | 12 | 42% | 58% |
| 7 Bilder-Upload<br>Content Sharing | 7.5 GB | 253 | 2 | 100% | 0% |
| 7 MasterDisk<br>Cloud Storage | 883.7 MB | 769 | 1 | 100% | 0% |
| 7 WikiSend<br>Cloud Storage | 263.7 MB | 147 | 11 | 100% | 0% |
| 7 PDFUnlock<br>Collaboration | 16.5 MB | 2 | 2 | 100% | 0% |
| 7 PDF Split<br>Collaboration | 12.6 MB | 18 | 1 | 100% | 0% |
| 7 freepdfconvert<br>Collaboration | 9.8 MB | 1 | 1 | 100% | 0% |
| 7 Fastupload<br>Cloud Storage | 8.8 MB | 1,083 | 675 | 0% | 100% |
| 7 PDF to DOCX<br>Collaboration | 8 MB | 1 | 1 | 100% | 0% |

# Analytics

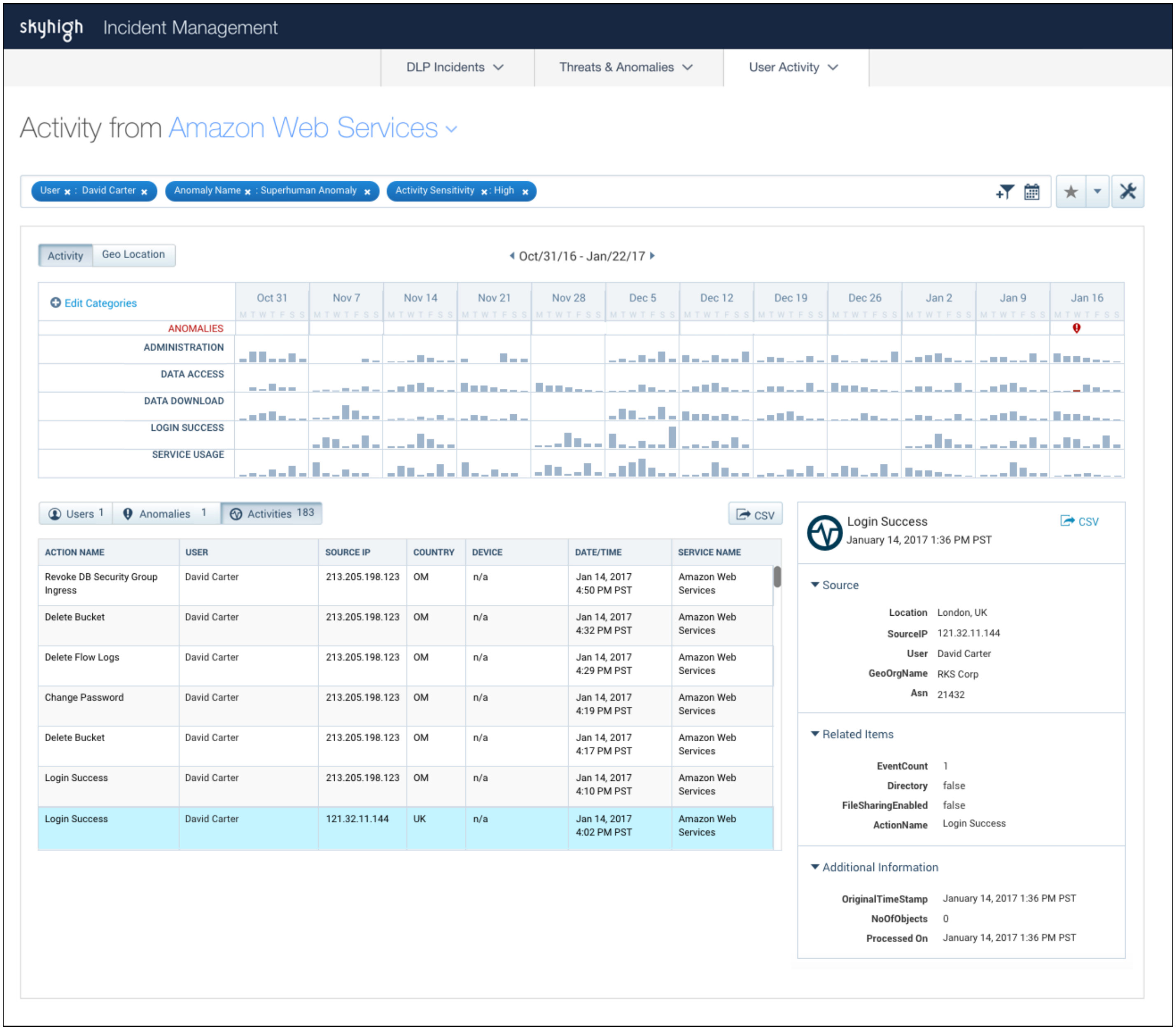
Skyhigh for AWS uses existing analytics capabilities, customized for AWS deployments:

- **Account Access Analytics.** Identifies inactive user accounts and former employees who retain access to AWS so their accounts can be deleted to reduce latent risk.
- **User Behavior Analytics.** Automatically builds a self-learning model based on multiple heuristics and identifies patterns of activity indicative of a malicious or negligent insider threat.
- **Privileged User Analytics.** Identifies excessive user permissions, inactive administrator accounts, inappropriate access to data, and unwarranted escalation of privileges and user provisioning.
- **Account Compromise Analytics.** Analyzes login attempts to identify impossible cross region access, brute-force attacks, and untrusted locations indicative of compromised accounts.

# Activity Monitoring

Activity Monitoring in Skyhigh for AWS means you'll be viewing activities within 10 minutes of an activity occurring (after being logged by CloudTrail).

Activities are categorized into commonly understood categories, meaning your information security team doesn't need to worry about each activity name. The Activity page also includes geo-locations of activities across accounts.



| ACTION NAME | USER | SOURCE IP | COUNTRY | DEVICE | DATE/TIME | SERVICE NAME |
|---|---|---|---|---|---|---|
| Revoke DB Security Group Ingress | David Carter | 213.205.198.123 | OM | n/a | Jan 14, 2017<br>4:50 PM PST | Amazon Web Services |
| Delete Bucket | David Carter | 213.205.198.123 | OM | n/a | Jan 14, 2017<br>4:32 PM PST | Amazon Web Services |
| Delete Flow Logs | David Carter | 213.205.198.123 | OM | n/a | Jan 14, 2017<br>4:29 PM PST | Amazon Web Services |
| Change Password | David Carter | 213.205.198.123 | OM | n/a | Jan 14, 2017<br>4:19 PM PST | Amazon Web Services |
| Delete Bucket | David Carter | 213.205.198.123 | OM | n/a | Jan 14, 2017<br>4:17 PM PST | Amazon Web Services |
| Login Success | David Carter | 213.205.198.123 | OM | n/a | Jan 14, 2017<br>4:10 PM PST | Amazon Web Services |
| Login Success | David Carter | 121.32.11.144 | UK | n/a | Jan 14, 2017<br>4:02 PM PST | Amazon Web Services |

Login Success
January 14, 2017 1:36 PM PST

Source

| | |
|---|---|
| Location | London, UK |
| SourceIP | 121.32.11.144 |
| User | David Carter |
| GeoOrgName | RKS Corp |
| Asn | 21432 |

Related Items

| | |
|---|---|
| EventCount | 1 |
| Directory | false |
| FileSharingEnabled | false |
| ActionName | Login Success |

Additional Information

| | |
|---|---|
| OriginalTimeStamp | January 14, 2017 1:36 PM PST |
| NoOfObjects | 0 |
| Processed On | January 14, 2017 1:36 PM PST |

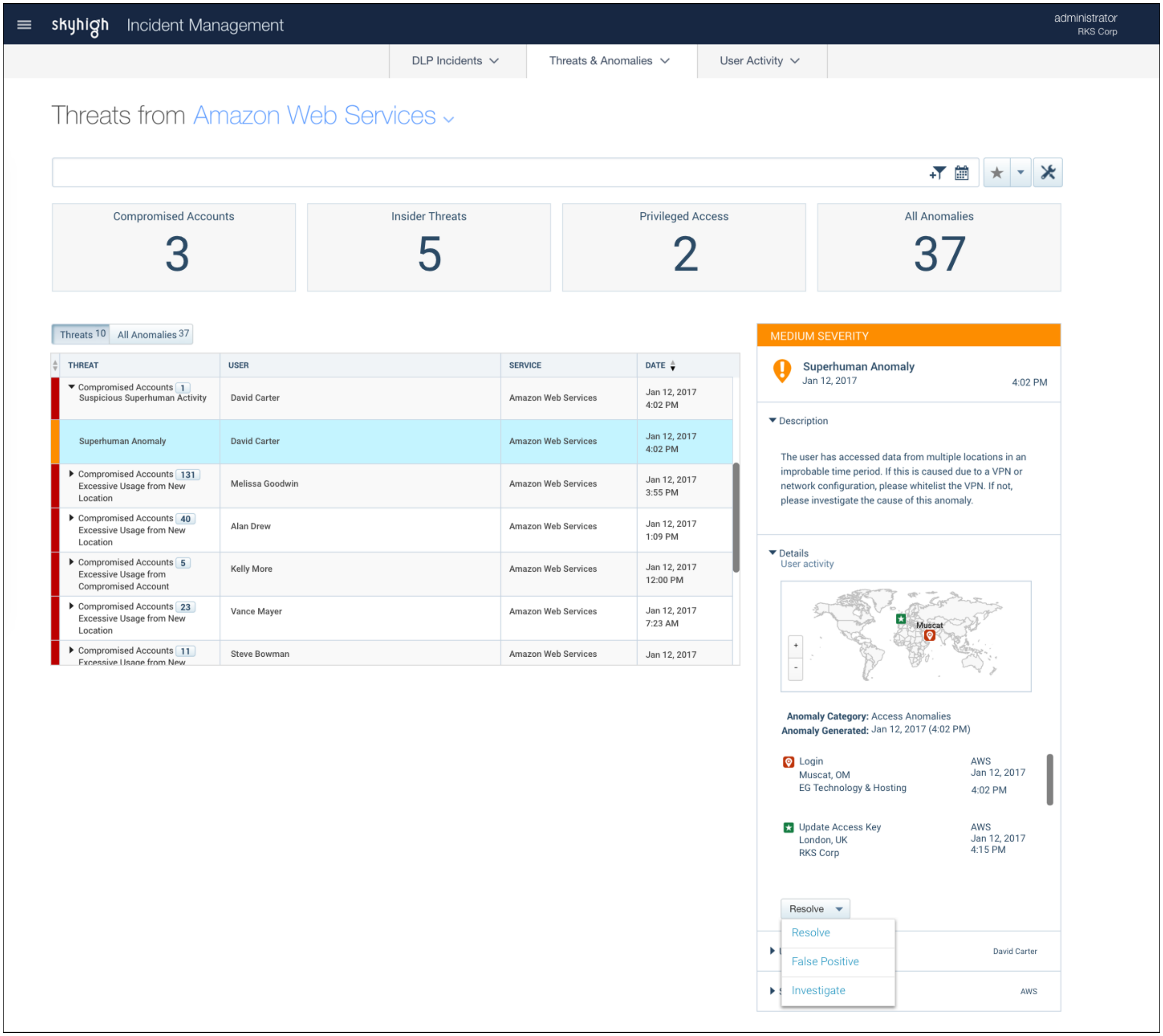
The Omnibar allows you to search and filter for activities by attributes such as user name, IP Address, City, Country, IP Organization, and more. You can download a set of activities in a CSV that can be submitted as forensic evidence.

## Threat Protection and Anomalies

Skyhigh for AWS detects compromised account threats, insider threats, and privileged access misuse threats. Skyhigh for AWS also ensures a SOC is not flooded by anomalies due to sudden changes in Skyhigh, AWS event feeds or bulk change patterns in usage.

Threat Protection optimizations for AWS include:

- Correlating multiple anomalous events within AWS or across AWS and other cloud services to accurately separate true threats from simple anomalies.
- Detecting anomalies in usage related to access to AWS, data on AWS or administration of AWS.
- Filtering false positives from anomalies based on machine learning and UEBA.
- Whitelisting of known "good" entities or acceptable risk for the enterprise.
- Throttling of events to accommodate bandwidth in the SOC team.



Threats from Amazon Web Services

| Compromised Accounts | Insider Threats | Privileged Access | All Anomalies |
|---|---|---|---|
| 3 | 5 | 2 | 37 |

Threats 10 | All Anomalies 37

| THREAT | USER | SERVICE | DATE |
|---|---|---|---|
| Compromised Accounts 1<br>Suspicious Superhuman Activity | David Carter | Amazon Web Services | Jan 12, 2017<br>4:02 PM |
| Superhuman Anomaly | David Carter | Amazon Web Services | Jan 12, 2017<br>4:02 PM |
| Compromised Accounts 131<br>Excessive Usage from New Location | Melissa Goodwin | Amazon Web Services | Jan 12, 2017<br>3:55 PM |
| Compromised Accounts 40<br>Excessive Usage from New Location | Alan Drew | Amazon Web Services | Jan 12, 2017<br>1:09 PM |
| Compromised Accounts 5<br>Excessive Usage from Compromised Account | Kelly More | Amazon Web Services | Jan 12, 2017<br>12:00 PM |
| Compromised Accounts 23<br>Excessive Usage from New Location | Vance Mayer | Amazon Web Services | Jan 12, 2017<br>7:23 AM |
| Compromised Accounts 11<br>Excessive Usage from New | Steve Bowman | Amazon Web Services | Jan 12, 2017 |

MEDIUM SEVERITY

Superhuman Anomaly
Jan 12, 2017 4:02 PM

Description

The user has accessed data from multiple locations in an improbable time period. If this is caused due to a VPN or network configuration, please whitelist the VPN. If not, please investigate the cause of this anomaly.

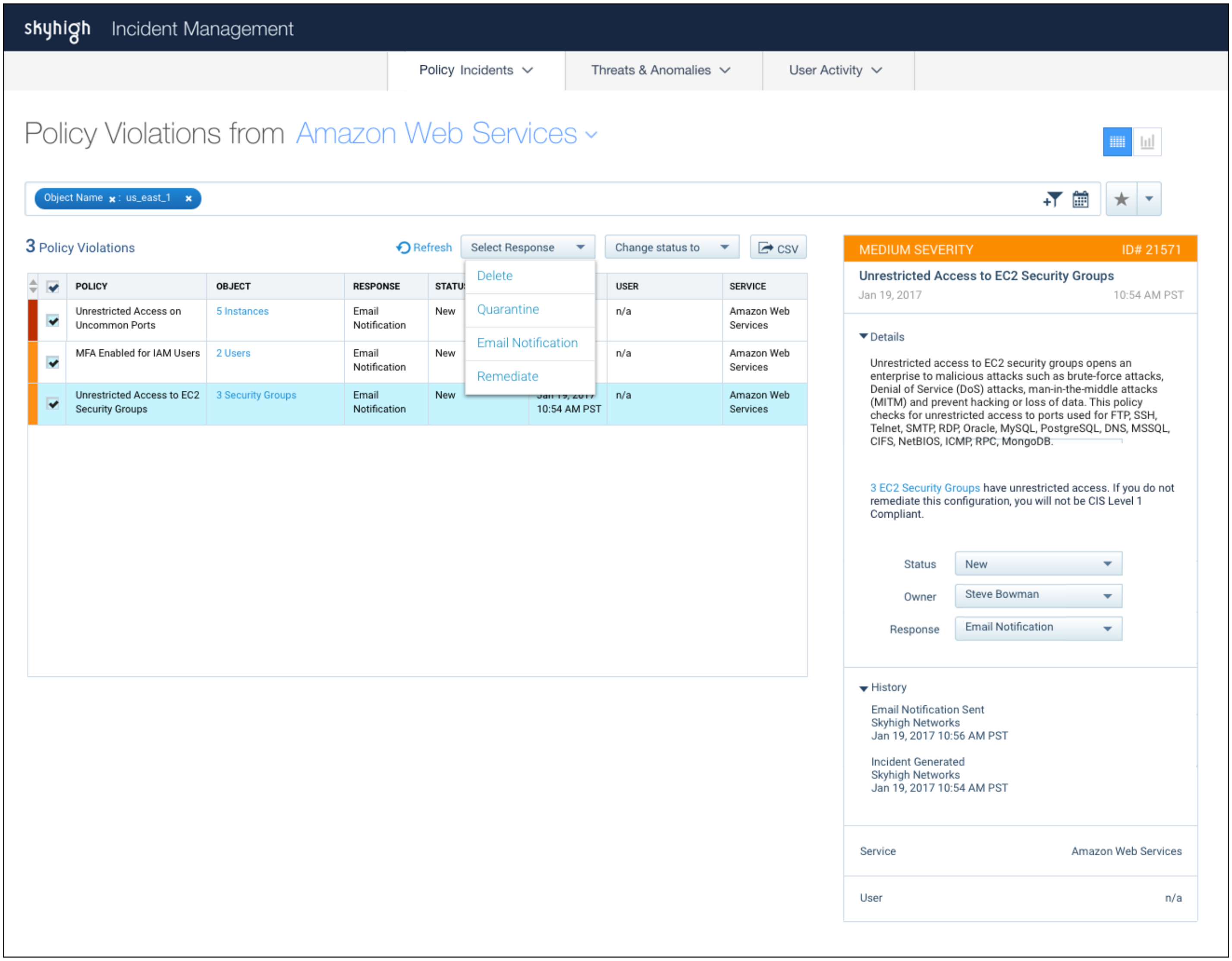
Details
User activity

**Anomaly Category:** Access Anomalies
**Anomaly Generated:** Jan 12, 2017 (4:02 PM)

| | |
|---|---|
| Login<br>Muscat, OM<br>EG Technology & Hosting | AWS<br>Jan 12, 2017<br>4:02 PM |
| Update Access Key<br>London, UK<br>RKS Corp | AWS<br>Jan 12, 2017<br>4:15 PM |

# Compliance Policies

Compliance Policies help you secure many different aspects of your AWS deployment. For a full list of policies, see Skyhigh Compliance Policies.



skyhigh Incident Management

Policy Incidents | Threats & Anomalies | User Activity

Policy Violations from Amazon Web Services

Object Name: us_east_1

3 Policy Violations

Refresh | Select Response | Change status to | CSV

Delete, Quarantine, Email Notification, Remediate

| ☑ | POLICY | OBJECT | RESPONSE | STATU |  | USER | SERVICE |
|---|---|---|---|---|---|---|---|
| ☑ | Unrestricted Access on Uncommon Ports | 5 Instances | Email Notification | New |  | n/a | Amazon Web Services |
| ☑ | MFA Enabled for IAM Users | 2 Users | Email Notification | New |  | n/a | Amazon Web Services |
| ☑ | Unrestricted Access to EC2 Security Groups | 3 Security Groups | Email Notification | New | Jan 19, 2017 10:54 AM PST | n/a | Amazon Web Services |

MEDIUM SEVERITY ID# 21571

Unrestricted Access to EC2 Security Groups

Jan 19, 2017 10:54 AM PST

Details

Unrestricted access to EC2 security groups opens an enterprise to malicious attacks such as brute-force attacks, Denial of Service (DoS) attacks, man-in-the-middle attacks (MITM) and prevent hacking or loss of data. This policy checks for unrestricted access to ports used for FTP, SSH, Telnet, SMTP, RDP, Oracle, MySQL, PostgreSQL, DNS, MSSQL, CIFS, NetBIOS, ICMP, RPC, MongoDB.

3 EC2 Security Groups have unrestricted access. If you do not remediate this configuration, you will not be CIS Level 1 Compliant.

Status New

Owner Steve Bowman

Response Email Notification

History

Email Notification Sent
Skyhigh Networks
Jan 19, 2017 10:56 AM PST

Incident Generated
Skyhigh Networks
Jan 19, 2017 10:54 AM PST

Service Amazon Web Services

User n/a

# Security Configuration Audit

Skyhigh for AWS monitors 30 configuration settings that increase the risk profile of AWS deployments across four categories:

- Security Monitoring
- Secure Authentication
- Unrestricted Access
- Inactive Entities

Skyhigh for AWS continuously monitors AWS configuration against regulatory requirements to streamline internal and external audits, such as ISO 27008, PCI, HIPAA, and so on.