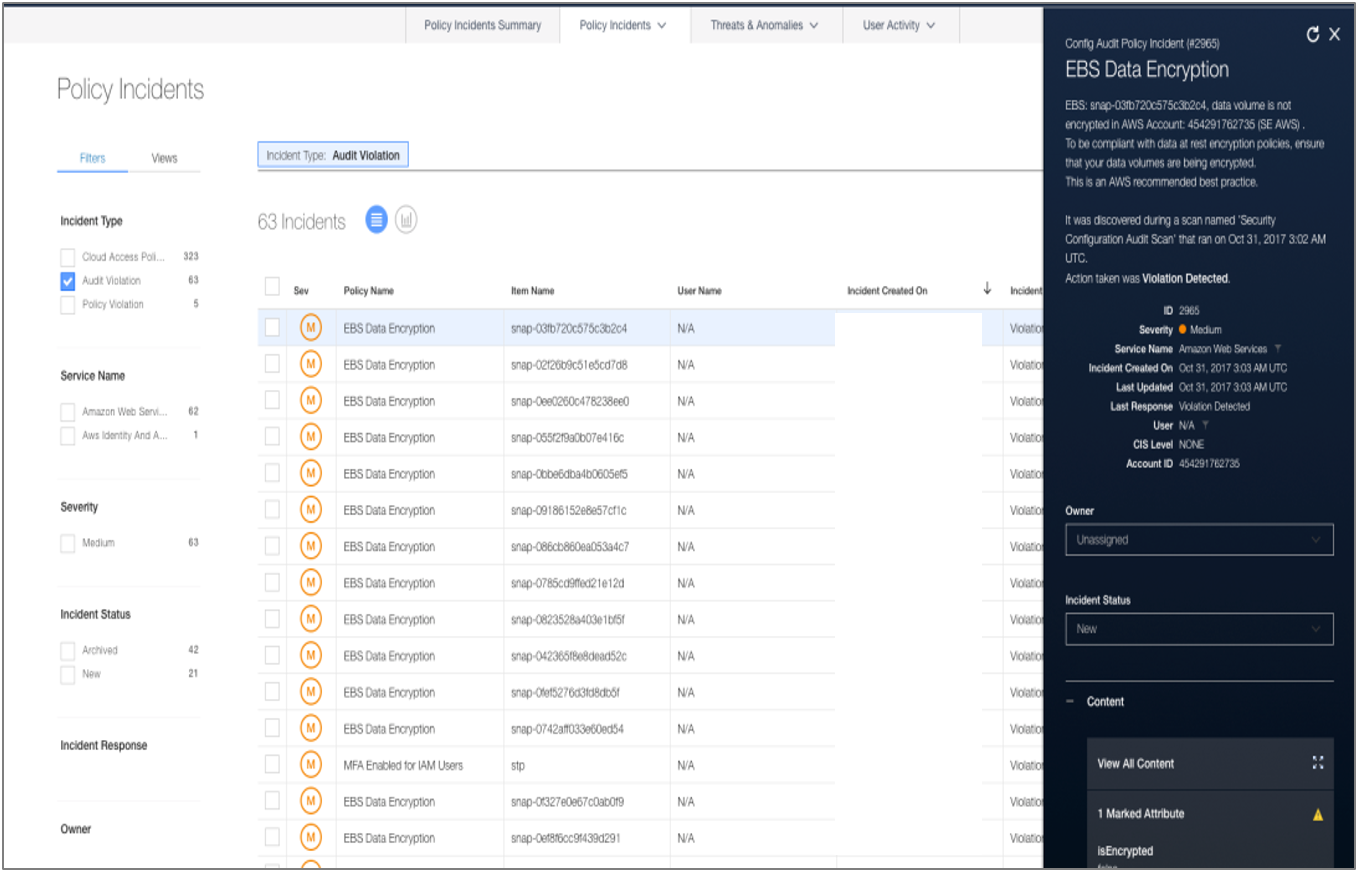
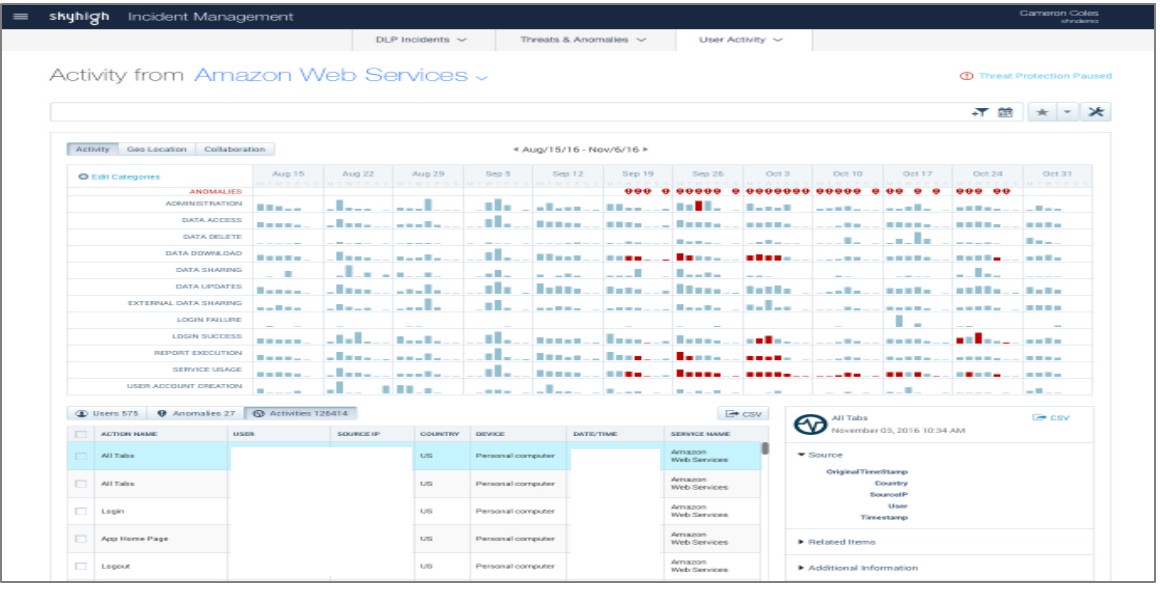
Skyhigh for AWS Use Cases

Audit IaaS Environments to Identify Unsecured/Noncompliant Configurations

* Discover current AWS security settings and suggests modifications to improve security
* Monitor security by enabling logging for AWS Cloud Trail
* Identify security loopholes such as unrestricted inbound access to ports
* Secure authentication by requiring MFA for the AWS root account, or modifications to security settings

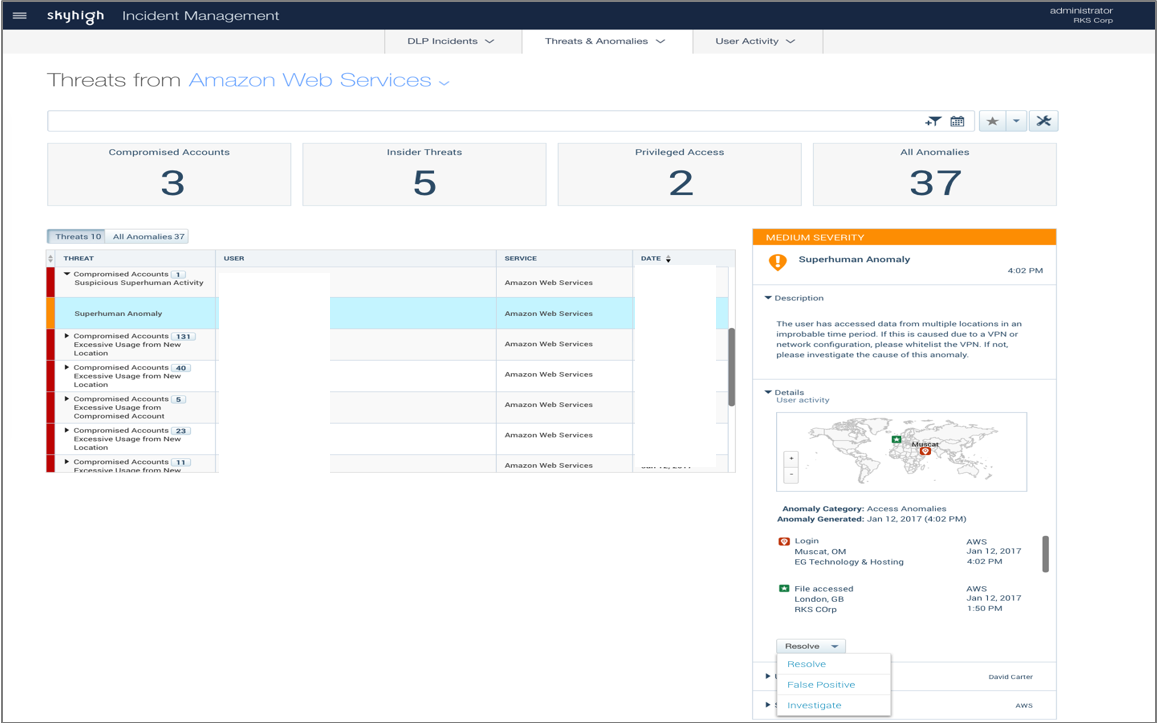


Monitor Activity and Create Audit Trail for Compliance and Investigations



Detect Insider and Privileged User Threats, Compromised Accounts

* Monitor all activities including escalation of privileges, user provisioning, and sensitive data access
* Leverage machine learning to detect insider and privileged user threat
* Utilize geolocation analysis to identify compromised accounts
* Access a threat protection dashboard and incident-response workflow to review and remediate potential threats



Deployment Configuration – Checklist

Feature/Component

* AWS Account
* Enterprise Connector - SIEM Integration and Active Directory Attribute based User Groups (Optional)
* User Provisioning

Readiness Item

* Setup roles for Skyhigh IAM user in all AWS accounts
* Cloud Trail logging setup to write to an S3 bucket.
* SIEM appliance (Splunk / QRadar)
* LDAP (AD / ADFS)
* VM to install Skyhigh Enterprise Connector
* Dashboard Users
* Support Portal Users