Symantec.

CloudSOC™

for Amazon Web Services

Security for Amazon Web Services (AWS)

Do you want to make sure your AWS accounts are secure and have not been compromised? What are your risks if a malicious insider or an external bad actor uses your AWS for their own purposes? Do you have the visibility and control you need to make sure this doesn't happen?

See how CloudSOC can keep your AWS accounts secure.

amazon web services

Detect and prevent threats based on patent-pending data science and machine learning

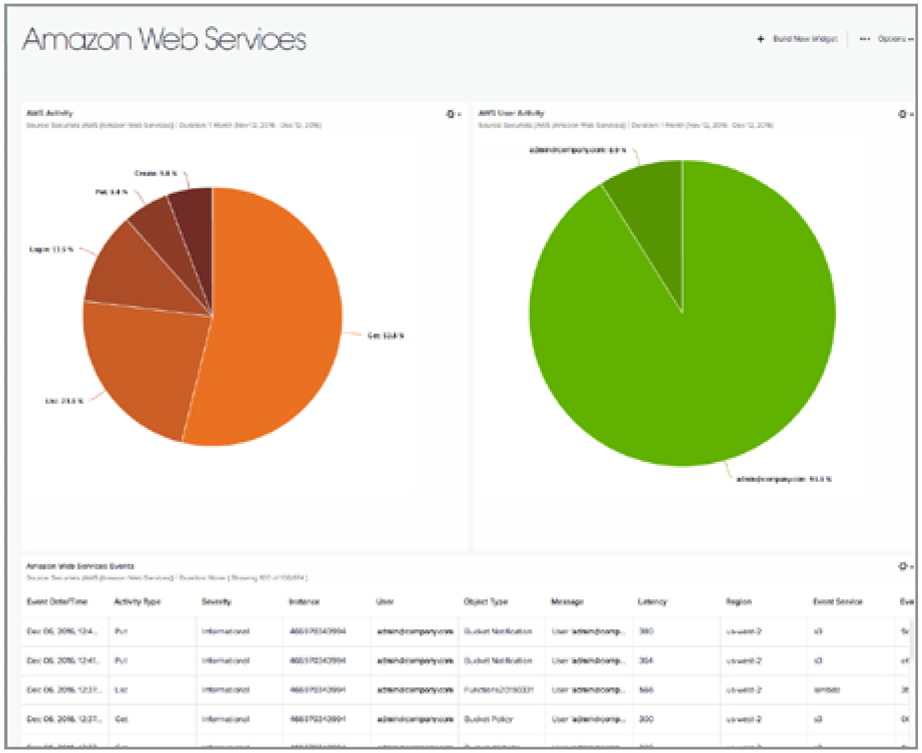
Enforce security policies to alert, mitigate and prevent security incidents

Investigate and respond to security incidents with powerful analysis tools based on granular log data

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Security Risk



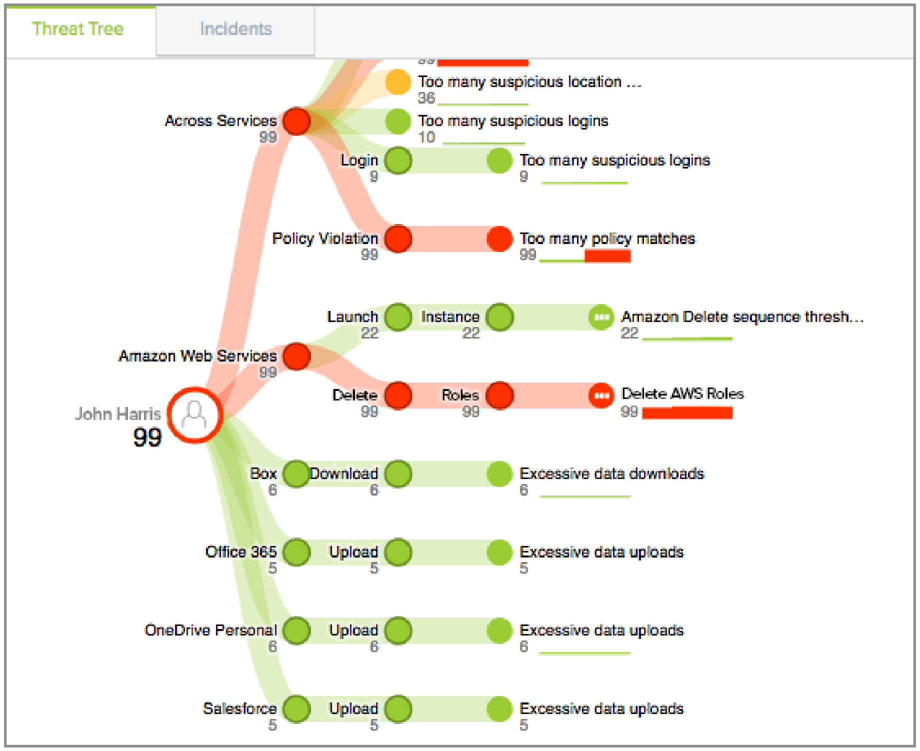
Amazon Web Services

Amazon Web Services Events

Event Date/Time	Activity Type	Severity	Instance	User	Object Type	Message	Latency	Region	Event Service
Dec 06, 2016, 12:4…	Put	Informational	466170340994	admin@company.com	Bucket Notification	User 'admin@comp…	380	us-west-2	s3
Dec 06, 2016, 12:41…	Put	Informational	466170340994	admin@company.com	Bucket Notification	User 'admin@comp…	304	us-west-2	s3
Dec 06, 2016, 12:37…	List	Informational	466170340994	admin@company.com	Functions20150331	User 'admin@comp…	566	us-west-2	lambda
Dec 06, 2016, 12:37…	Get	Informational	466170340994	admin@company.com	Bucket Policy	User 'admin@comp…	300	us-west-2	s3

Monitor users and action in AWS to quickly identify and act on abnormal or malicious activity.

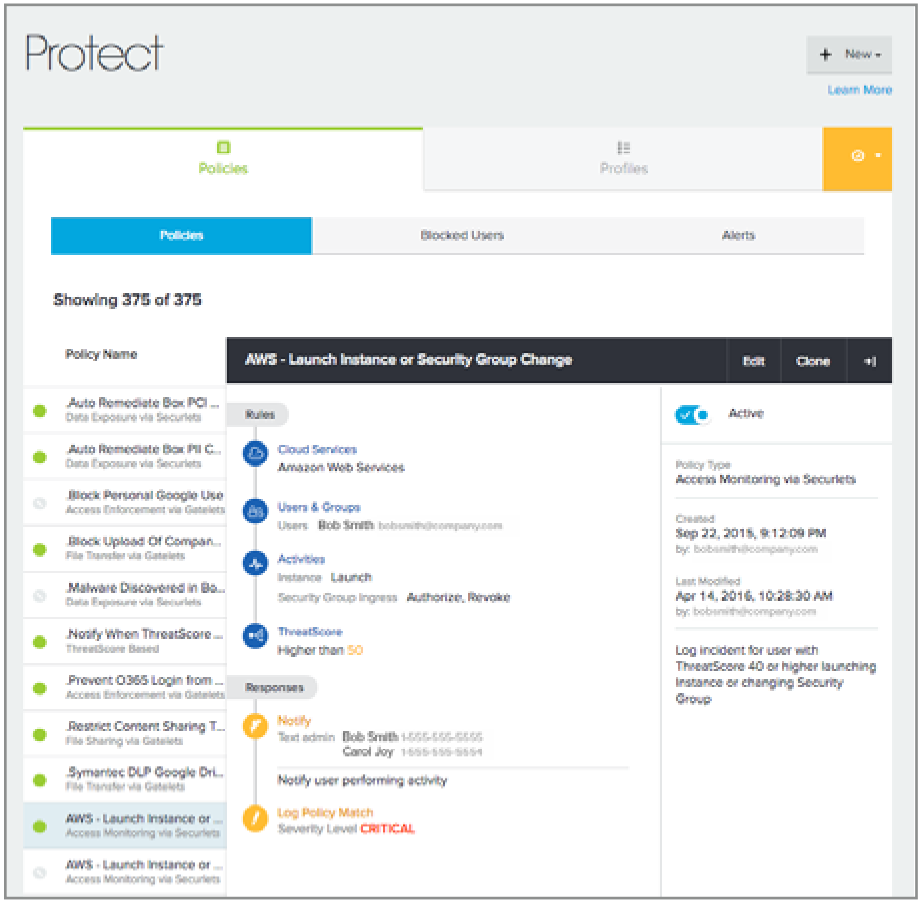
User Centric ThreatScore



Account takeovers and malicious insiders can put your organization at risk. Machine learning based User Behavior Analysis assigns a ThreatScore to each and every user, enabling you to identify and act on risky users.

Safeguard your AWS account from hackers and malicious insiders using your infrastructure for their purposes. Identify malicious activity and eliminate unsanctioned activities, virtual machines and servers.

Policy Definition



Protect

+ New ▾

Learn More

Policies | Profiles

Policies | Blocked Users | Alerts

Showing 375 of 375

	Policy Name
●	.Auto Remediate Box PCI ... Data Exposure via Securlets
●	.Auto Remediate Box PII C... Data Exposure via Securlets
○	.Block Personal Google Use Access Enforcement via Gatelets
●	.Block Upload Of Compan... File Transfer via Gatelets
○	.Malware Discovered in Bo... Data Exposure via Securlets
●	.Notify When ThreatScore ... ThreatScore Based
●	.Prevent O365 Login from ... Access Enforcement via Gatelets
●	.Restrict Content Sharing T... File Sharing via Gatelets
●	.Symantec DLP Google Dri... File Transfer via Gatelets
●	AWS - Launch Instance or ... Access Monitoring via Securlets
○	AWS - Launch Instance or ... Access Monitoring via Securlets

AWS - Launch Instance or Security Group Change | Edit | Clone

Rules

Cloud Services
Amazon Web Services

Users & Groups
Users Bob Smith bobsmith@company.com

Activities
Instance Launch
Security Group Ingress Authorize, Revoke

ThreatScore
Higher than 50

Responses

Notify
Text admin Bob Smith 1-555-555-5555
Carol Joy 1-555-555-5554

Notify user performing activity

Log Policy Match
Severity Level CRITICAL

Active

Policy Type
Access Monitoring via Securlets

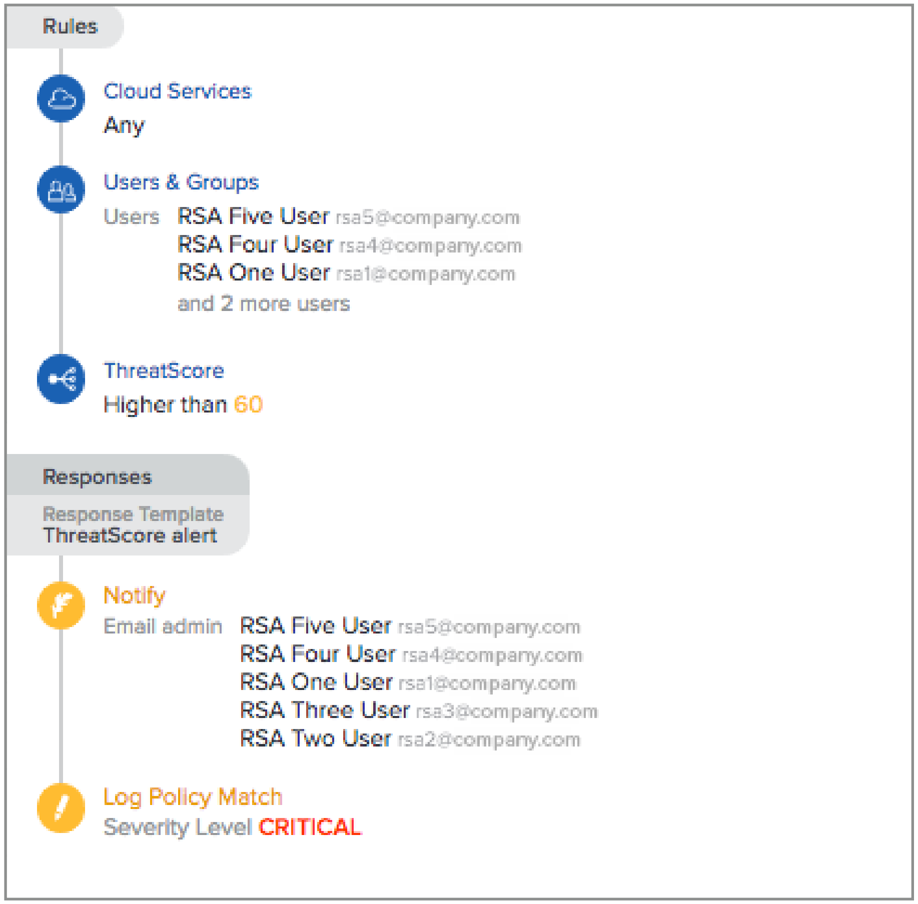
Created
Sep 22, 2015, 9:12:09 PM
by: bobsmith@company.com

Last Modified
Apr 14, 2016, 10:28:30 AM
by: bobsmith@company.com

Log incident for user with ThreatScore 40 or higher launching Instance or changing Security Group

Define security policies to automatically alert and remediate risks as they occur and prevent unsanctioned activity.

Real-time Enforcement



Rules

Cloud Services
Any

Users & Groups
Users RSA Five User rsa5@company.com
RSA Four User rsa4@company.com
RSA One User rsa1@company.com
and 2 more users

ThreatScore
Higher than 60

Responses

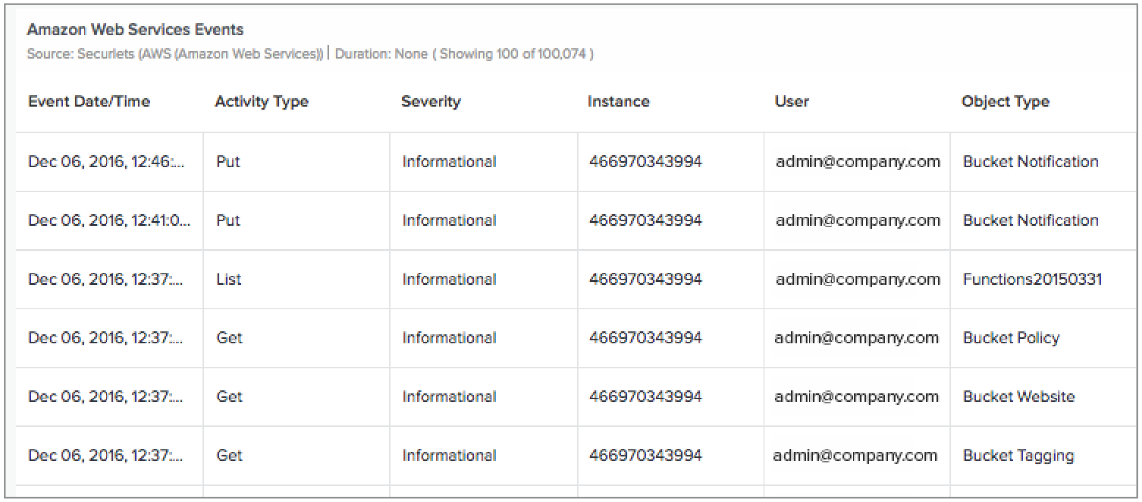
Response Template
ThreatScore alert

Notify
Email admin RSA Five User rsa5@company.com
RSA Four User rsa4@company.com
RSA One User rsa1@company.com
RSA Three User rsa3@company.com
RSA Two User rsa2@company.com

Log Policy Match
Severity Level CRITICAL

Prevent security incidents with real-time enforcement policies triggered by elevated ThreatScores.

Incident Response



Amazon Web Services Events

Source: Securlets (AWS (Amazon Web Services)) | Duration: None (Showing 100 of 100,074)

Event Date/Time	Activity Type	Severity	Instance	User	Object Type
Dec 06, 2016, 12:46:...	Put	Informational	466970343994	admin@company.com	Bucket Notification
Dec 06, 2016, 12:41:0...	Put	Informational	466970343994	admin@company.com	Bucket Notification
Dec 06, 2016, 12:37:...	List	Informational	466970343994	admin@company.com	Functions20150331
Dec 06, 2016, 12:37:...	Get	Informational	466970343994	admin@company.com	Bucket Policy
Dec 06, 2016, 12:37:...	Get	Informational	466970343994	admin@company.com	Bucket Website
Dec 06, 2016, 12:37:...	Get	Informational	466970343994	admin@company.com	Bucket Tagging

Go back in time and investigate a specific user or activity, correlate events and discover what really happened with powerful search and data visualization tools or export granular log data to your SIEM system for analysis.

Peace of mind comes when CloudSOC is watching over your AWS account to safeguard your assets and your organization.

It's easy to get going! Just connect to CloudSOC Security for AWS. Get the AWS Securlet API, you will have visibility and control over your AWS account in minutes. Add the CASB Gateway with the AWS Gatelet for additional levels of security.

More information

To speak with a Product Specialist in the U.S.
Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.
For specific country offices and contact numbers, please visit our website **symantec.com**

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings — anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 19,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2015, it recorded revenues of $6.5 billion. **To learn more go to www.symantec.com or connect with Symantec at: http://www.symantec.com/social/**