Symantec

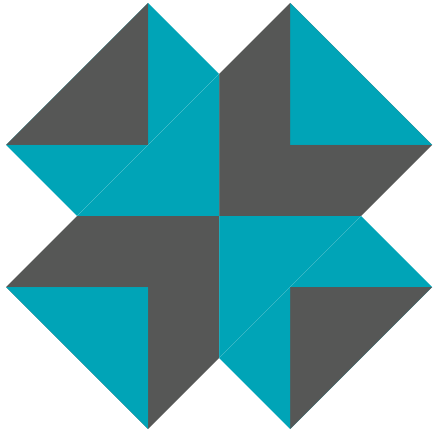
Symantec CloudSOC™ Data Science

Feature Brief Series 04

Detect, UBA, & ThreatScore

User Behavior Analytics

Catch attacks and high risk users fast



What if your CASB automatically identified high risk users and compromised accounts? What if you could diagnose what's going on with those accounts at a glance?

CloudSOC automatically identifies high risk users and compromised accounts enabling automated responses and fast resolution of security issues

What is CloudSOC UBA?

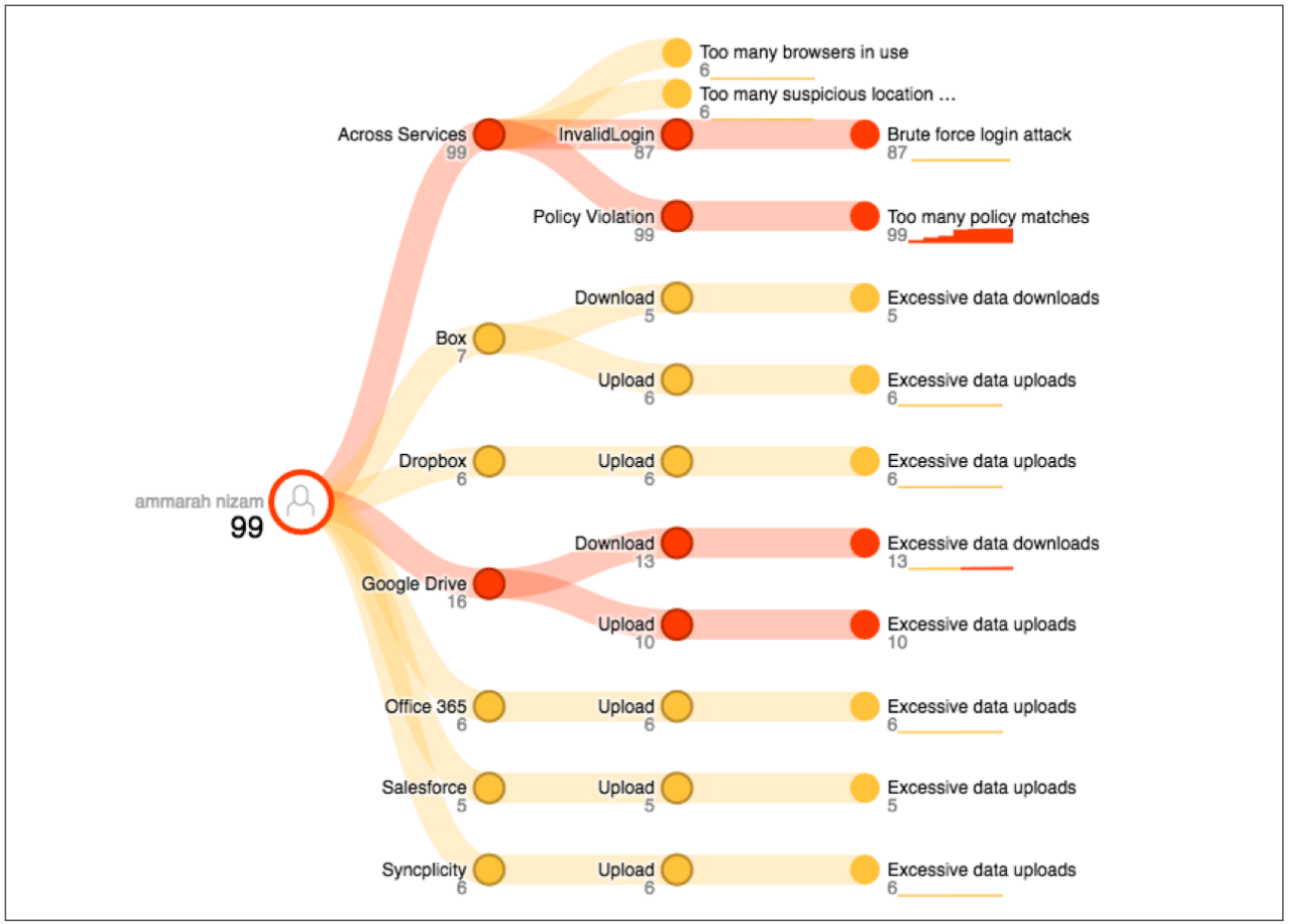
CloudSOC leverages a data science driven User Behavior Analytics (UBA) capability that automatically tracks user activity, assesses a risk level for that activity, and assigns a ThreatScore to each user and user action. CloudSOC UBA delivers the intelligence foundation for the Detect dashboard, provides details in CloudSOC Investigate incident records, and can be used to automatically trigger policy responses with CloudSOC Protect. As a result, CloudSOC delivers:

- **Automatic detection of high risk users, compromised accounts, and malicious insiders**
- **Individualized ThreatScore for fast identification of problem users**
- **Threat maps with granular detail for at-a-glance risk analysis and diagnosis**
- **Analysis of behavior for specific apps and across multiple apps in context for both sanctioned and unsanctioned accounts**
- **Automated policy controls for users triggered with an elevated ThreatScore**
- **Customizable detection settings for behaviors, thresholds, threats, and events**
- **Detection of high risk sequences of events using a combination of sanctioned corporate cloud accounts and unsanctioned personal cloud accounts**

Quickly Detect and Diagnose High Risk User Accounts

CloudSOC includes a Detect dashboard that automatically identifies high risk users and potentially compromised user accounts. This dashboard also displays a visual map of high risk actions in context for each user to enable at-a-glance diagnoses of likely problems.

The UBA engine in CloudSOC automatically assigns each user a continually updated ThreatScore based on individualized user behavior profiles. The Detect dashboard automatically displays users with the highest ThreatScores at the top of the list. With one click you can see a visual threat map representation of the actions performed by that user, color coded by risk level. Often a quick glance at the threat map is all it takes to understand what kind of situation you may have -- from data exfiltration attempts to malware infections to brute force attacks. From the threat map it is easy to drill down into the details of security incidents or click over to see how this risky activity compares to normal behavior patterns for this user.



The Data Science of CloudSOC UBA and ThreatScore

CloudSOC uses machine learning with expansive cloud processing and storage resources to power a self-training UBA engine. UBA algorithms develop a confidence curve for normal behavior customized to individual users in context with specific actions, apps, and other attributes to create and maintain collections of highly accurate user behavior profiles. CloudSOC uses computational analysis of user behavior to identify and score the severity of incidents and then correlates this use score with threshold-defined triggers and detection of suspicious sequences of events to calculate the dynamic ThreatScore for each user and action.

The machine learning approach in CloudSOC enables more accurate identification of risky activity in cloud apps, delivering a solution with:

- **Better awareness of abnormal activity due to more granular understanding of typical user behavior,**
- **Fewer false positives through individualized and contextualized user behavior modeling,**
- **Faster response capabilities leveraging automated ThreatScore calculations.**

The Benefits of CloudSOC UBA

Automatically detect risky users and abnormal activity

CloudSOC assigns each user an automated individual user ThreatScore. The Detect dashboard prominently displays the users with the highest ThreatScores so you instantly know who represents high risk and abnormal activity.

Diagnose problem accounts at-a-glance

CloudSOC automatically creates a visual map of activity for each user, color coded to represent risk levels. These Threat Maps provide incident information in context for each user, helping make it possible to diagnose a situation at-a-glance.

Automate policy controls and protective responses

You can create automated policy responses in CloudSOC based on user ThreatScore, thresholds, DLP violations or threat detections to control access, prevent data exfiltration or destruction, prevent proliferation of malware, and more.

Fast and accurate incident investigations

Security incident detection adds to the richness in incident records in the CloudSOC Investigate dashboard making it faster and easier to discover what has happened in order to successfully resolve a security incident.

More from the CloudSOC Data Science Feature Brief Series

01

Cloud App Intelligence

CloudSOC Business Readiness Ratings™
Extensive, accurate, timely intelligence on thousands of cloud apps

02

ContentIQ™ DLP

CloudSOC ContentIQ™
Extremely accurate, automated DLP with ContentIQ

03

StreamIQ™ Automation

CloudSOC StreamIQ™
New apps, custom apps, any apps with StreamIQ

04

Detect with UBA

CloudSOC ThreatScore™
Catch attacks and high risk users fast

Better Security, Less Complexity

Deploy a cloud security solution that integrates with your existing security infrastructure. A Symantec solution with CloudSOC provides greater security coverage, reduces operational complexity, and provides an optimal user experience.

Explore Symantec CloudSOC CASB and its industry leading integrations with Symantec Enterprise Security Systems go.symantec.com/casb

About CloudSOC

The Data Science Powered™ CloudSOC platform empowers companies to confidently leverage cloud applications and s ervices while staying safe, secure and compliant. A range of capabilities delivers the full life cycle of cloud application security, including auditing of shadow IT, real-time detection of intrusions and threats, protection against intrusions and compliance violations, and investigation of historical account activity for post-incident analysis.

About Symantec

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™

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

Symc_FB_CloudSOC_DataScienceSeries_en_v1d