Solution Brief

Symantec® and Fortinet® Security Solution

Joint Solution Components

- Fortinet FortiSOAR
- Symantec CloudSOC CASB

Joint Solution Benefits

- Monitor, govern, protect, and place policy controls on sanctioned and unsanctioned cloud accounts
- Data loss prevention (DLP) with automated data classification to prevent accidental or malicious loss of confidential data
- Harness user and entity behavior analytics (UEBA) and unparalleled threat protection for automated detection of malicious insiders, attacks, and advanced threats
- Streamlined operational efficiency through custom automated framework that pulls together all of the organization's tools
- Multimode oversight using native cloud application programming interfaces (APIs), real-time traffic processing, and input from numerous data feeds

A Comprehensive Solution for Cloud App Visibility, Data Security, and Threat Protection and Response

Executive Summary

Broadcom and Fortinet have partnered to deliver an industry-leading security solution by integrating the Symantec CloudSOC® platform and FortiSOAR® to provide enterprises with full visibility into cloud applications, enable threat information sharing and timely detection of threats for enforcement, and contain and thwart them in their path.

Challenge

Many security teams struggle to keep up with the pace of alerts and enforcements. Their challenges include having too many consoles to monitor, alert overload, reliance on manual processes, and a shortage of cybersecurity personnel. Adding to their challenges is an effort to extend traditional security to the cloud. Cloud accounts are often accessible directly from the internet, introducing a new threat vector. Bad actors target user accounts to gain direct access to sensitive content and infiltrate an organization. Users connecting to accounts with malware-infected devices can inadvertently infect the broader organization or cause a data breach.

Joint Solution

Broadcom and Fortinet have partnered to deliver an industry-leading solution to address these challenges. The integration of the Symantec CloudSOC and Fortinet FortiSOAR solutions enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem facilitates efficient investigation of alerts, allowing security analysts to better understand, review, and manage data in the cloud and on-premises, as well as to detect and generate alerts independently via its other integrations (for example, with security information and event management [SIEM] platforms) and use that information to enforce administrative actions within CloudSOC.

Joint Solution Components

FortiSOAR: A holistic and enterprise-built security orchestration and security automation workbench that empowers security operations teams. FortiSOAR increases a team's effectiveness by increasing efficiency, allowing for response in near real time.

Symantec CloudSOC CASB: Symantec CloudSOC provides visibility, data security, and threat protection for today's cloud generation of users across a wide range of sanctioned and unsanctioned apps. A range of capabilities on the CloudSOC platform delivers the full life cycle of cloud application security, including auditing of shadow IT, user behavior detection, real-time detection of intrusions and threats, protection against data loss, as well as examination and prevention of compliance violations and historical account activity for post-incident analysis.

Joint Solution Integration

The Symantec CloudSOC and Fortinet FortiSOAR joint solution operates to mitigate threat levels and high-risk activity of a user.

Use Case 1

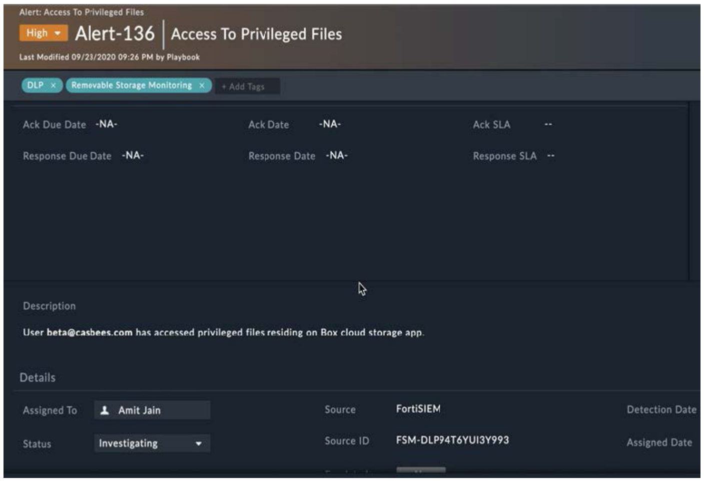
FortiSOAR consumes threat information from CloudSOC via API and enforces policies within the Fortinet Security Fabric. FortiSOAR generates an alert once it detects that a user has accessed privileged files (Figure 1). FortiSOAR will consult with CloudSOC and retrieve information on this user's threat risk.

The Symantec CloudSOC UEBA solution component analyzes alerts and telemetry from diverse security sources to connect the dots between violations, users, accounts, and assets. A core data science engine uses machine learning (ML) to create individualized user behavior profiles, and in combination with threshold and sequence detectors, can identify a risk level for each user and each incident. The user risk levels and incident risk levels are aggregated into a numerical ThreatScore for easy identification of problem incidents and high-risk users. This comparative risk scoring helps to detect and identify malicious insiders and outsiders and deliver rapid prioritization of user and entity-based alerts that represent emerging risks across multiple platforms, along with categorizing those incidents tied to misaligned policies or user mistakes.

FortiSOAR obtains this information from Broadcom via its API and can enforce three actions within its platform:

- FortiSOAR can mark the user as suspicious.
- It can disable the risky user in AD.
- It can raise the level of the alert to "critical."

Figure 1: Alert Within FortiSOAR upon a Breach



Alert: Access To Privileged Files

High Alert-136 | Access To Privileged Files

Last Modified 09/23/2020 09:26 PM by Playbook

DLP × Removable Storage Monitoring × + Add Tags

Ack Due Date -NA- Ack Date -NA- Ack SLA --

Response Due Date -NA- Response Date -NA- Response SLA --

Description

User beta@casbees.com has accessed privileged files residing on Box cloud storage app.

Details

Assigned To: Amit Jain

Status: Investigating

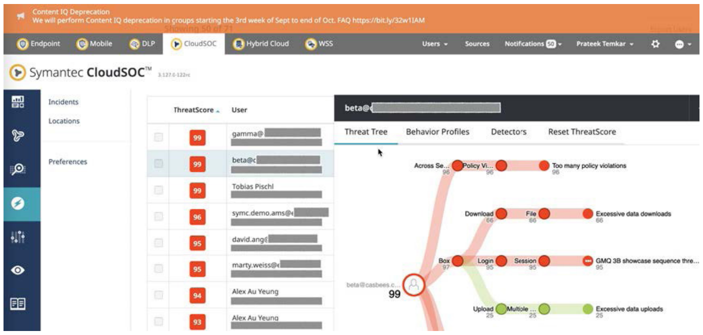
Source: FortiSIEM

Source ID: FSM-DLP94T6YUI3Y993

Detection Date

Assigned Date

Figure 2: The CloudSOC UEBA Engine Determines that this User is Risky and Assigns a High Threat Score of 99



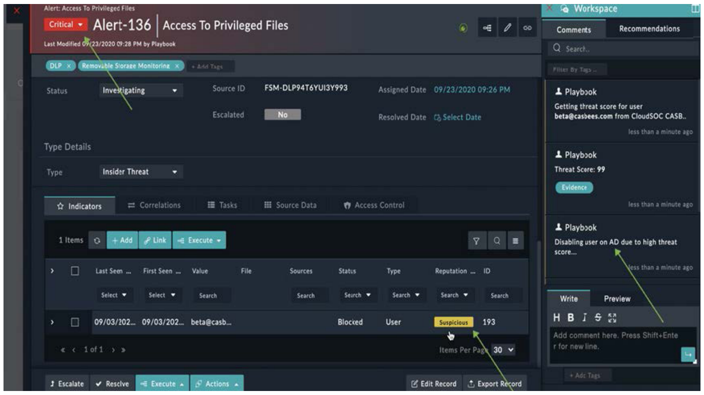
Content IQ Deprecation
We will perform Content IQ deprecation in groups starting the 3rd week of Sept to end of Oct. FAQ https://bit.ly/32w1IAM

beta@[redacted]

ThreatScore	User
99	gamma@[redacted]
99	beta@c[redacted]
99	Tobias Pischl [redacted]
96	symc.demo.ams@[redacted]
95	david.ang[redacted]
95	marty.weiss@[redacted]
94	Alex Au Yeung [redacted]
93	Alex Au Yeung [redacted]

beta@casbees.c...
99
Across Se... 96
Policy Vi... 96
Too many policy violations 96
Download 66
File 66
Excessive data downloads 66
Box 97
Login 95
Session 95
GMQ 3B showcase sequence thre... 95
Upload 25
Multiple ... 25
Excessive data uploads 25

Figure 3: FortiSOAR Can Enforce Three Actions within its Platform



Alert: Access To Privileged Files

Critical Alert-136 | Access To Privileged Files

Last Modified 09/23/2020 09:28 PM by Playbook

DLP × Removable Storage Monitoring × + Add Tags

Status: Investigating

Source ID: FSM-DLP94T6YUI3Y993

Assigned Date: 09/23/2020 09:26 PM

Escalated: No

Resolved Date: Select Date

Type Details

Type: Insider Threat

Last Seen ...	First Seen ...	Value	File	Sources	Status	Type	Reputation ...	ID
09/03/202...	09/03/202...	beta@casb...			Blocked	User	Suspicious	193

Playbook
Getting threat score for user beta@casbees.com from CloudSOC CASB..
less than a minute ago

Playbook
Threat Score: 99
Evidence
less than a minute ago

Playbook
Disabling user on AD due to high threat score...
less than a minute ago

Use Case 2

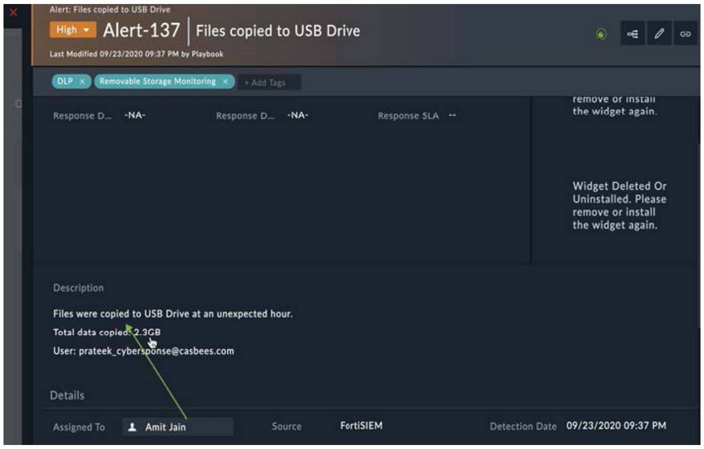
The FortiSOAR-CloudSOC API integration can also be leveraged to enforce administrative action within CloudSOC. In a data leakage incident, FortiSOAR generates an alert (Figure 4) and notifies the admin to approve the deactivation of the user in CloudSOC (Figure 5).

Once approved, the user will be deactivated in CloudSOC (Figure 6).

Summary

While the expansion into the cloud has many benefits, security and data privacy professionals are being challenged to provide security and governance for cloud applications. The Broadcom and Fortinet partnership extends the traditional security functions to protect sensitive data that is prevalent in the cloud environment. The combination of the Symantec CloudSOC with Fortinet FortiSOAR accomplishes this through visibility, data security, and threat protection for cloud users across a wide range of sanctioned and unsanctioned apps, resulting in faster responses and streamlined containment for reduced mitigation times.

Figure 4: An Alert Generated by FortiSOAR upon Detection of Data Breach and Leakage



Alert: Files copied to USB Drive

High Alert-137 | Files copied to USB Drive

Last Modified 09/23/2020 09:37 PM by Playbook

DLP × Removable Storage Monitoring × + Add Tags

Response D... -NA- Response D... -NA- Response SLA --

remove or install the widget again.

Widget Deleted Or Uninstalled. Please remove or install the widget again.

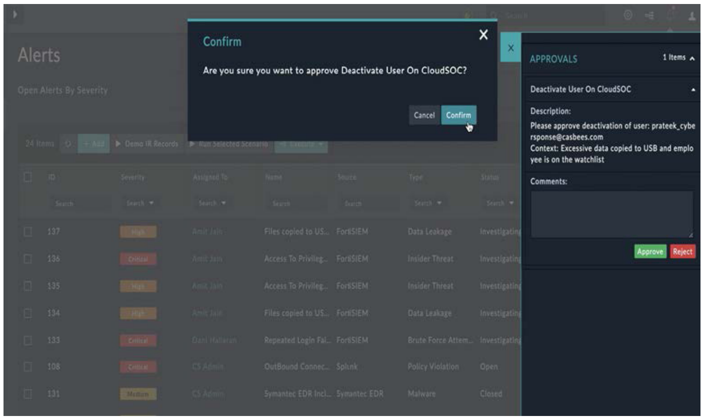
Description

Files were copied to USB Drive at an unexpected hour.
Total data copied: 2.3GB
User: prateek_cybersponse@casbees.com

Details

Assigned To: Amit Jain Source: FortiSIEM Detection Date: 09/23/2020 09:37 PM

Figure 5: FortiSOAR Notifies the Admin to Approve the Deactivation of the User in CloudSOC



Alerts

Open Alerts By Severity

Confirm

Are you sure you want to approve Deactivate User On CloudSOC?

Cancel Confirm

APPROVALS 1 Items

Deactivate User On CloudSOC

Description:
Please approve deactivation of user: prateek_cybersponse@casbees.com
Context: Excessive data copied to USB and employee is on the watchlist

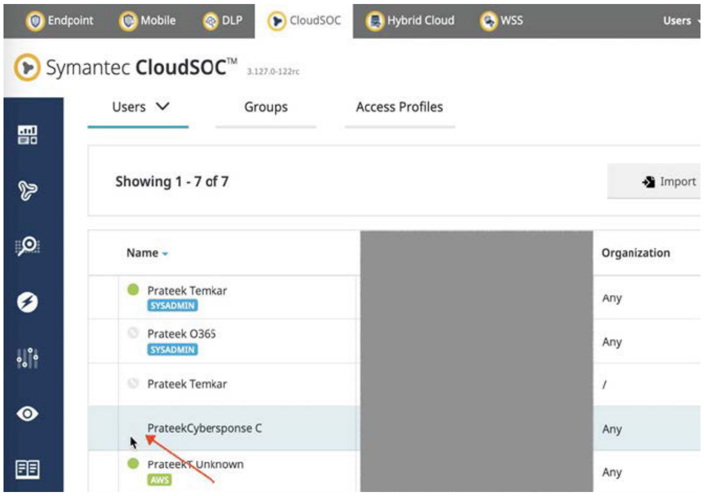
Comments:

Approve Reject

24 Items + Add ▶ Demo IR Records ▶ Run Selected Scenario

ID	Severity	Assigned To	Name	Source	Type	Status
137	High	Amit Jain	Files copied to US...	FortiSIEM	Data Leakage	Investigatin
136	Critical	Amit Jain	Access To Privileg...	FortiSIEM	Insider Threat	Investigatin
135	High	Amit Jain	Access To Privileg...	FortiSIEM	Insider Threat	Investigatin
134	High	Amit Jain	Files copied to US...	FortiSIEM	Data Leakage	Investigatin
133	Critical	Dani Halloran	Repeated Login Fai...	FortiSIEM	Brute Force Attem...	Investigatin
108	Critical	CS Admin	OutBound Connec...	Splunk	Policy Violation	Open
131	Medium	CS Admin	Symantec EDR Inci...	Symantec EDR	Malware	Closed

Figure 6: Deactivation of User Through the CloudSOC Console



Symantec CloudSOC™ 3.127.0-122rc

Users Groups Access Profiles

Showing 1 - 7 of 7 Import

Name	[redacted]	Organization
Prateek Temkar SYSADMIN		Any
Prateek O365 SYSADMIN		Any
Prateek Temkar		/
PrateekCybersponse C		Any
Prateek Unknown AWS		Any

For product information and a complete list of distributors, visit our website at: broadcom.com