Solution Brief

Sophos Integrations: Identity

Detect and respond to suspicious user activity

Sophos' 2024 State of Ransomware report highlights that compromised credentials are the root cause of ransomware attacks in 29% of incidents. Implementing multi-factor authentication is critical for mitigating unauthorized access. Sophos XDR and MDR integrations with identity providers enable security analysts to discover malicious activity and active adversaries masquerading as legitimate users.

Use Cases

1 | IDENTIFY ACCOUNT COMPROMISE

Desired Outcome: Uncover authentication-related issues, including brute force attacks, credential stuffing, and attempts to bypass multi-factor controls.

Solution: Early detection of adversaries attempting to exploit compromised credentials is crucial to prevent the exposure of sensitive data and systems. Insider threats and unauthorized use by employees or contractors pose significant risks. Sophos XDR and MDR integrations with identity providers enable analysis of security events, ensuring fast remediation of post-exploit activities.

2 | DETECT ABNORMAL GEOLOCATION LOGINS

Desired Outcome: Discover unusual logins to identify illicit access.

Solution: Geolocation tracking enables systems to detect logins from atypical locations. Sophos' Identity integrations capture telemetry to identify untrusted or unenrolled endpoints, invalid or disabled assets, and blacklisted zones. Detect unauthorized access by correlating historical data with real-time activity across protected assets within the network.

3 | STOP AND RESPOND TO CREDENTIAL ABUSE

Desired Outcome: Prevent ongoing access by credentials harvested to establish persistence.

Solution: Attackers move laterally using stolen login credentials, targeting devices that evade detection. Leveraging data from your identity platform, security analysts identify compromised accounts, confirm breaches, and execute response actions to disrupt attacker access, including host-based account lockouts, suspending users, resetting user passwords, and more.

4 | SUPPORT COMPLIANCE REQUIREMENTS

Desired Outcome: Monitor and report irregular logins as mandated by regulatory standards.

Solution: Collecting alerts from identity solutions enables you to meet requirements of regulatory standards, including GDPR and HIPAA, shielding your organization from potential legal and financial consequences. As an optional add-on, Sophos allows ingested log data to be retained for up to 365 days for all Sophos XDR and MDR integrations.

Integrations include

Microsoft DUO

okta Auth0

and more.

G2 Leader

Named a Leader in XDR in the G2 Summer 2024 Reports

Gartner Peer Insights Customers' Choice 2023™

A Customers' Choice in the 2023 Gartner®, Voice of the Customer for Managed Detection and Response Services report

To learn more, visit
www.sophos.com/mdr
www.sophos.com/xdr

Gartner, Voice of the Customer for Managed Detection and Response Services, 28 July 2023. The Gartner Peer Insights Logo is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

SOPHOS