← Case report for event ID: 8816

ID	Alert rule	Description	Incident type	Severity level	Date and time detected
8816	Access to Blacklisted External URL Blocked by Firewall	This alert was triggered when a user attempted to access an external URL that is listed in the organization's blacklist or threat intelligence feeds. The firewall or proxy successfully blocked the outbound request, preventing the connection. Note: The blacklist only covers known threats. It does not guarantee protection against new or unknown malicious domains.	Firewall	High	Nov 30th 2025 at 12:18

Alert details

datasource: firewall

timestamp: 11/30/2025 04:15:50.186

Action: blocked

SourceIP: 10.20.2.17

SourcePort: 34257

DestinationIP: 67.199.248.11

DestinationPort: 80

URL: http://bit.ly/3sHkX3da12340

Application: web-browsing

Protocol: TCP

Rule: Blocked Websites

Incident report

Edit report

Incident classification

(●) True positive ( ) False positive

Case report

Please write a detailed report on the steps taken to analyse and contain this incident, including all relevant information and the rationale for its closure.

Time of activity: 11/30/2025 04:15:50.186

List of Affected Entities:
datasource: firewall
timestamp: 11/30/2025 04:15:50.186
Action: blocked
SourceIP: 10.20.2.17
SourcePort: 34257
DestinationIP: 67.199.248.11
DestinationPort: 80
URL: http://bit.ly/3sHkX3da12340
Application: web-browsing

Reason for Classifying as True Positive:
- The user was accessing the blocked website through a web browser and was blocked by the firewall
- The website may contain unsafe cache and cookies, and connections (and specific reasons on why it is blocked)

Does this alert require escalation?

(●) Yes ( ) No

Complete IR:

Time of activity: 11/30/2025 04:15:50.186

List of Affected Entities:

datasource: firewall

timestamp: 11/30/2025 04:15:50.186

Action: blocked

SourceIP: 10.20.2.17

SourcePort: 34257

DestinationIP: 67.199.248.11

DestinationPort: 80

URL: http://bit.ly/3sHkX3da12340

Application: web-browsing

Reason for Classifying as True Positive:

- The user was accessing the blocked website through a web browser and was blocked by the firewall
- The website may contain unsafe cache and cookies, and connections (and specific reasons on why it is blocked)

Reason for Escalating the Alert:

- The user needs to explain why the blocked website was attempted to access
- Destination port is 80 - http - unsafe

Recommended Remediation Actions:

- policy reminder

- background checking of the user (can be an insider or shadow IT)

List of Attack Indicators:

- Attempt to access blocked website

- Destination port is 80 - http - unsafe