Integrating MS Teams and Palo Alto Networks Panorama or Firewalls

Overview

Sun Management is a Palo Alto Networks Partner, Palo Alto Networks Certified Services Partner, and Palo Alto Networks Authorized Training Center. Our Engineers have designed and installed over $100M in Palo Alto Firewall Security since 2009. As a Palo Alto Networks Authorized Training Center we have trained over 2000 students on effective utilization of the Palo Alto Networks Firewall. As such, we aim to provide continuous access to on-going training for our existing clients, potential clients and any other individual interested in further develop of their engineering skills with Palo Alto Networks Firewalls.

Organizations using MS Teams have opportunities to leverage MS Teams to receive high-priority notifications from your Palo Alto Networks Panorama (or firewalls). In this walk through I'll show you how easy it is to set that up in MS Teams and on your Palo Alto Networks firewall and to tailor the alerts to what is important to and urgent for your organization.

The Scenario

You want to team members to get notification in MS Teams for certain alerts from your Panorama (or your firewall if you don't use Panorama). The alerts forwarded to MS Teams are defined in a filter (or multiple filters) on the firewall, tailored to the requirements of your organization. Examples include threat log entries with severity critical; wildfire submissions with verdict malicious; or correlated events, configuration or system log entries of particular interest. I'll use Correlated Events of high or critical severity as the alerts I'm interested in getting alerts about in MS Teams.

Using MS Teams with targeted notification from Palo Alto Networks Panorama provides a way to reduce alert fatigue while keeping your team informed about relevant critical alerts.

Prep work in MS Teams

In MS Teams you need a channel, and then on that channel you are going to add an incoming webhook. Setting up the webhook gives you a webhook URL in a format like

https://yourcompany.webhook.office.com/webhookb2/xxxxxxxc1a8@61a6xxxx83b/IncomingWebhook/677d099cxxxxxxxxxxxxxxxxxxa1/4303xxxxxxxxxxxxxxxxxxx4b17

You need that webhook URL for the channel or channels you want to post in, and that incoming webhook is tied to a particular channel in MS Teams.

See the link in the resources section for instructions about configuring MS Teams.

On the Palo Alto Networks Panorama

High level steps on Panorama for notification for correlated events:

1. Setup the HTTP server profile

2. Configure a logging destination

3. Commit your changes

4. Revise formatting and query as needed until it is what you want

Step by step on Panorama for Correlated Events log event notification:

1. Setup the HTTP server profile. Go to Panorama > Server Profiles > HTTP and click Add.

a. Use the dialog to create a new profile named MS Teams Post

b. Click Add at bottom to add a new server, using the info below:

Name: Teams post

Address: <first part of webhook URL from above, without https://>

Example: yourcompany.webhook.office.com

Protocol: HTTPS

Port 443

TLS 1.2

Certificate profile: none

HTTP method: POST

Here is what it looks like once that profile is created and the server is added:

c. Next, go to the Payload Format tab

For Correlation log, click on “Correlation” under the Log Type and use these settings

Name: MS Teams Correlation log post

URI Format: /webhookb2/the rest of your webhook URL from MS Teams

HTTP Headers:

Headers: content-type

Value: application/json

No Parameters

For Payload, start with what is shown below, and modify as needed after testing, depending on your environment. (cut and paste to a text editor to remove any formatting, including the opening and closing curly brackets)

*** start of payload ***

```
{
        "@type": "MessageCard",
        "@context": "https://schema.org/extensions",
        "summary": "Critical-High Correlation Event",
        "themeColor": "0078D7",
        "title": "Panorama Alerting: $object_name",
        "sections": [
                {
                        "activityTitle": "$srcuser",
                        "activitySubtitle": "$time_generated",
                        "facts": [
                                {
                                        "name": "Source user:",
                                        "value": "$srcuser"
                                },
                                {
                                        "name": "Severity:",
                                        "value": "$severity"
                                },
                                {
                                        "name": "Type:",
                                        "value": "$type"
                                },
```

```
                {
                        "name": "Category:",
                        "value": "$category"
                }
            ],
            "text": "This user was found in a correlation event log entry of high or critical severity."
        }
    ]
}
```


*** end of payload ***

Press OK twice to save changes and exit config dialog.

d. Open the HTTP Server profile you just saved, then on the second tab, go into the MS Teams Correlation Log post and use the Send Test Log button to see if it can submit to MS Teams. It may take 30 seconds or more to return the result. You should see it in your MS Teams channel within a minute.

e. If you get an error or it fails to show in MS Teams

a. check the traffic log to see if you have denied traffic from the firewall management interface (by default, or from specified interface if using service routes). Hint: view the traffic log using the filter "(app eq MS Teams-base) and (addr.src in <your firewall mgmt. port IP Address>)" to see those submissions.

b. Check formatting of the payload

f. Once the test post shows in MS Teams, proceed with next step.

Screenshot below of what it looks like in Teams, obviously the variables will be replaced with data from the log entry once there is a matching log entry to generate the post.

2. Configure Log forwarding. Because this is a "system" log not a "traffic related" log, we aren't going to use a log forwarding profile like we would with Wildfire or Threat logs on a firewall. Go to Panorama > Log Settings (or on a firewall Device > Log Settings).

a. Scroll down to the bottom and find Correlation, click Add

Name: Correlation log critical or high <or whatever is descriptive for your setup>

Description: forward any correlation log entries that are high or critical

Filter: (severity eq high) or (severity eq critical) <or whatever is appropriate for your organization, use the filter builder as needed>

Forward method: go to HTTP, click Add, then select MS Teams Post from drop down

Click OK twice to save changes

3. Commit your changes

4. Test and revise as needed to generate notifications for the events you want to see in MS Teams, and to provide useful information in the body of the notification.

The example above is for notification from the Correlation log, from Panorama or a PAN-OS firewall. Depending on the log you are interested in getting alerted on and whether or not you are using Panorama, setting up other logs may be the same or you could need to setup a Log Forwarding Profile, which is then referenced in the Security Policies on the firewall. See our writeup on using Slack integration for step by step process to forward events from traffic/threat logs on a PAN-OS firewall.

Next Steps

If you want to implement this in your environment and would be more comfortable having someone with experience help you in the process, contact your Sun Management account rep to schedule one of our certified Palo Alto Networks engineers to assist with setting up notification from the firewalls into MS Teams.

If you want to test this on your own and do not have access to a lab environment to do so, contact your Sun Management account rep to get pricing on a lab bundle. The PA-220 and VM-50 appliances are excellent platforms for testing things such as this and there are specific part numbers for lab equipment that are more heavily discounted than the same appliance for use in production.

Sun Management

Sun Management is a Value Added Reseller (VAR) focusing on Network and Internetwork Security Requirements. We work primarily in the Mid Atlantic area: Maryland (MD), Virginia (VA), District of Columbia (DC), West Virginia (WV), Delaware (DE) and Pennsylvania (PA). Our credentials include Palo Alto Networks Services Provider, Palo Alto Networks Certified Training Partner, and Palo Alto Networks Certified Managed Security Service Provider (MSSP) using CORTEX XSOAR in a multi-tenant environment.

We address requirements concerning Network Detection and Response (NDR); internal and external TLS and SSL requirements for complete data visibility; End Point Detection and Response (EDR); Gramm Leach Bliley Act, HIPPA, Sarbanes Oaxley and PCI DSS; penetration testing and firewall optimization; and Data Protection by tracking all Data Flows within the network, across applications, between users/servers and in the cloud. Contact us at (888) 773-9422 to setup a POC or if you just want more

Resource Links

https://docs.microsoft.com/en-us/microsoftteams/platform/webhooks-and-connectors/how-to/add-incoming-webhook (how to setup incoming webhook and some concepts)

https://live.paloaltonetworks.com/t5/log-forwarding-articles/pan-os-8-0-http-log-integration-with-slack/ta-p/172093 (written for Slack but adapted here for MS Teams)

https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/monitoring/forward-logs-to-an-https-destination.html (log forwarding to http destination)

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFfCAK

https://messagecardplayground.azurewebsites.net/ (some examples for formatting MS Teams posts)