Enabling Security Information Sharing

Nancy Cam-Winget, Syam Appala and Scott Pope

Cisco Systems Inc, San Jose CA

Abstract

Security event analysis, classification and response is easier when you have all the facts, especially if those facts are timely and accurate. But when it comes to answering simple forensics questions like "who is this security event associated with and what level of access do they have on the network" and "what type of device is this security event coming from", those facts are often difficult to come by; and even when they are available, they are often wrong or out of date making the incident classification and response process time-consuming.

With industry trends requiring the sharing of security events, there is a need to provide an ecosystem to facilitate the information flow securely. This paper describes one such implementation: pxGrid.

What is pxGrid?

The Platform Exchange Grid (pxGrid) is an XMPP based unified framework developed by Cisco that enables ecosystem participants to integrate to pxGrid once, then share context either uni or bidirectionally with many platforms without the need to adopt platform-specific APIs. pxGrid is secure and customizable, enabling partners to share only what they want to share and consume only context relevant to their platform.

Key features of pxGrid include:

- Ability to control what context is shared and with which platforms – Because pxGrid is customizable, partners can "publish" only the specific contextual information they want to share and can control the partner platform that information gets shared with.

- Bidirectional context sharing – pxGrid enables platforms to both share or publish context as well as consume or "subscribe to" context from specific platforms. These features are orchestrated and secured by the pxGrid server.

- Ability to share context data in native formats – Contextual information shared via pxGrid is done in each platform's native data format.

- Ability to connect to multiple platforms simultaneously – pxGrid enables

platforms to publish only the context data relevant to partner platforms. Numerous context "topics" may be customized for a variety of partner platforms, yet always shared via the same reusable pxGrid framework. Furthermore, only sharing relevant data enables both publishing and subscribing platforms to scale their context sharing by eliminating excess, irrelevant data.

Example use cases leveraging pxGrid

This section highlights two use cases leveraging pxGrid.

Use Case 1: Fine-grain control access in a federated environment

Current federated solutions such as Ping ID or Ping Federate currently affect authentication and authorization through the use of a single identity. With the use of pxGrid, collaboration and sharing of network information, identity context (e.g. device type, location) and (network) policy attributes, finer grain access controls can now be affected.

Beyond the improvements that are brought to the user by a single sign-on experience, the information shared between network access control systems and Identity solutions access control to web assets based on risk level can now also be realized.

Use Case 2: Improving Security Insight and Actionable Intelligence

Enabling the sharing of information from the network to SIEM vendors improves the visibility and efficacy of visibility, vulnerability and threat detection. NetIQ currently leverages identity and network information through pxGrid to improve on their security analysis and enable them to answer queries such as "who is this event associated with and what level of access do they have on the network" and "what type of device is it coming from" all within the NetIQ Sentinel management console.

Summary

pxGrid is an XMPP based secure means by which information can be shared to improve on security events and solutions. More details of pxGrid can be found in www.cisco.com/c/.../at_a_glance_c45-728420.pdf and as the proposed controller and transport in IETF's Secure Automation and Continuous Monitoring (SACM) working group as https://datatracker.ietf.org/doc/draft-salowey-sacm-xmpp-grid/.