

G2DA Additional Workflow Risk Assessment Module for Tufin SecureChange

Introduction

The G2DA Additional Workflow Risk Assessment Module is a plug in module to Tufin SecureChange that augments and enhances existing Tufin functionality. The G2AWRAM is designed to easily calculate and display USP (unified security policy) compliance violations that are introduced as a result of changes introduced by workflows other than Access Requests in Tufin SecureChange.

Challenge

The Tufin group change, server clone, and rule modification functionality provides the powerful ability to easily modify and provision changes to monitored access control devices. This allows operations personnel to efficiently execute a repeatable and fully auditable process for introducing this type of change into the access control realm.

The challenge becomes understanding whether this type of change will introduce access policy changes that violate compliance policies defined for the infrastructure. A network object group change effects the apparent access control everywhere that group appears in an access control policy, whether it appears in the source, destination or both locations in a rule. Similarly, a server network access being cloned or a direct rule modification can introduce similar risk.

Although the Access Request mechanism in SecureChange calculates compliance policy violations for a fully formed access request (source, destination, service), this feature is not available natively for additional workflows.

Without calculating the compliance policy risk status of these additional workflows, operators could be introducing risk everywhere these workflows touch the access control policy.

Solution: The G2DA Additional Workflow Risk Assessment Module

The G2DA Additional Workflow Risk Assessment Module is a combination of purpose built software as well as integration with the Tufin SecureChange workflow mechanism. It works by calculating the USP risk associated with all rules changed by a group object modification or other workflow. The main purpose is to determine the risks associated with this type of change before these changes are implemented.

All rules that violate an existing USP as a result of any change are clearly displayed in the GUI. The operator can choose to simply cancel the change, or accept the risk as an exception and optionally inject the exception into the USP.

Edited

Device: **CP SMC**

Group: **PCI_DB**

Name	Type	IP/Group Members
db01	Host	10.200.1.220/255.255.255.255
db02	Host	10.200.1.221/255.255.255.255
ExchangeF5-LTM	Group	ex02 , ex01 , ex03
db03	Network	10.200.1.222/255.255.255.254
db04	Address Range	[10.200.1.224 - 10.200.1.226]

Edited

Device: **ASAv**

Group: **Sales**

Name	Type	IP/Group Members
vpn_172.16.30.100	Host	172.16.30.100/255.255.255.255
vpn_172.16.30.101	Host	172.16.30.101/255.255.255.255
Sales_192.168.2.100	Host	192.168.2.100/255.255.255.255
Sales_192.168.2.101	Host	192.168.2.101/255.255.255.255
DC_network	Network	10.200.1.0/255.255.255.0

Risk Summary

On device "**CP SMC**"

Modification of group "**PCI_DB**" violates USP "**PCI US Retail**" from zone "**NY Users**" to zone "**PCI DB**"

Rule 17 with name "mobile users access to **PCI 01**"

Rule 22 with name "mobile users access to **PCI 02**"

On device "**ASAv**"

Modification of group "**Sales**" violates USP "**Corporate Best Practices**" from zone "**DC Main Office**" to zone "**Sales VPN**"

Rule 15 with name "Sales **VPN** Access"

EXCEPTIONS

Find Matching Rules

Exception Name	Domain	Expiration Date	Creation Date	Created by	Requested by	Approved By	Ticket ID	Description
Exception for DC Network	All Domains	Tuesday, 1 April 2070	Friday, 1 April 2016	admin	John Doe	Ben Stern	313	Automatic Exception created by G2 Risk Assessment Module

When coupled with the G2DA Advanced Object handler, a separately available module, the network group change functionality extends to service object group changes. This risk assessment calculation can be implemented in any desired step or in multiple steps for that matter. For more info on how to purchase and implement the G2GORAM, please email info@g2da.com or call 617-834-5365.