01

AUTOMATE YOUR BLOCKLISTS

SOAR with Sentinel and Check Point

Thomas Dang, CISM, OSEP

Security Systems Architect, Yukon Government

CPX 2024 Las Vegas

02

whoami

- Security Architect at a sub-national government in Canada
- Organization with 5000+ employees and dozens of remote sites
- Software and Computer Science background with an interest in automating the boring and hard stuff
- DEF CON 32 War Stories speaker
- Former elected Member of the Legislature in Alberta, Canada

03

Automate your block lists in SecureXL for performance

Access Control Policies and Dynamic Objects are convenient and fast to implement.
What happens when your firewall can’t keep up? We saw a DDoS attack overwhelm the CPU and take down both firewalls.

04

Options

Let's compare all the ways we can implement IP block listing.

When list sizes are large and performance is a concern - we need to use the least convenient option.

Network Objects/ Dynamic Objects (opendbl.net)	Convenient/easy to update *High Performance Impact*
SAMP rules (sk103154)	Ready made script *Moderate Performance Impact*
Custom IoC Feed (sk132193)	Convenient/easy to update *High Performance Impact*
SecureXL Block list (sk112454)	Updated via clish/expert mode *Low Performance Impact*

05

Azure Sentinel and SOAR Solution

Samples

Setup SIEM and Azure Hybrid Workers to trigger on alerts

You must have a working Sentinel and Hybrid Worker environment with firewall log ingestion and integration to logic apps and runbooks.

Authentication/Service Accounts

Setup an RBAC role for a service account that only has access to SecureXL clish, no web access is necessary. SSH keys must be installed for a service account from the firewalls to your runbook server.

Automation Scripts to Synchronize Block lists

Azure hybrid runbooks are utilized to send block information back from Sentinel to the on-premise block lists. Scripts on Gaia expert mode are configured to synchronize block lists from runbook server.

06

Azure Security Considerations

- Use best practices when configuring your runbooks and automations.
- Use managed identities when possible, exercise the principles of least privilege.

Permissions Sample

07

Service Account Considerations

- Use SSH keys instead of static passwords.
- Exercise least privilege and only allow sftp for synchronization tools.
- Configure RBAC on Gaia to allow only least-privileged access. (SecureXL commands)

Service Account Sample

08

Links and references

Scripts used in this demo:
https://github.com/litobro/cpx-sentinel-automate

Find me:
https://thomasdang.ca

This builds on the work of Franesco Ficarola
https://www.francescoficarola.com/check-point-automated-ip-blacklist-v2/