While you wait…

Why not let us know what topics you'd like us to cover next?

Take the short survey at:

squaredup.com/topics

SquaredUp

Coffee Break Webinar Series

Community Resource – Security Monitoring MP

Topic

Nathan Gau's free Security Monitoring SCOM MP

Discussion points:

- What is it?
- Getting it configured
- Alert management strategy

Security Monitoring MP

A SCOM pack that provides real time notifications to security events that are worth investigation

“At that time (2015-2016) it was noted that attacker is in an organization on average for about 250 days before they are found”

“Organizations that prioritize security spend large amounts of money on big data tools like Splunk or OMS in conjunction with SCOM and Azure PowerBI, but these take an extensive time investment, training, and in some cases rare resources, and that’s before considering that you actually have to know what you’re looking for. ”

https://blogs.technet.microsoft.com/nathangau/2017/05/01/introducing-the-security-monitoring-management-pack-for-scom

Security Monitoring MP

Mainly tracks events that should occur rarely or not at all, in order to minimize noise and cry wolf behaviour

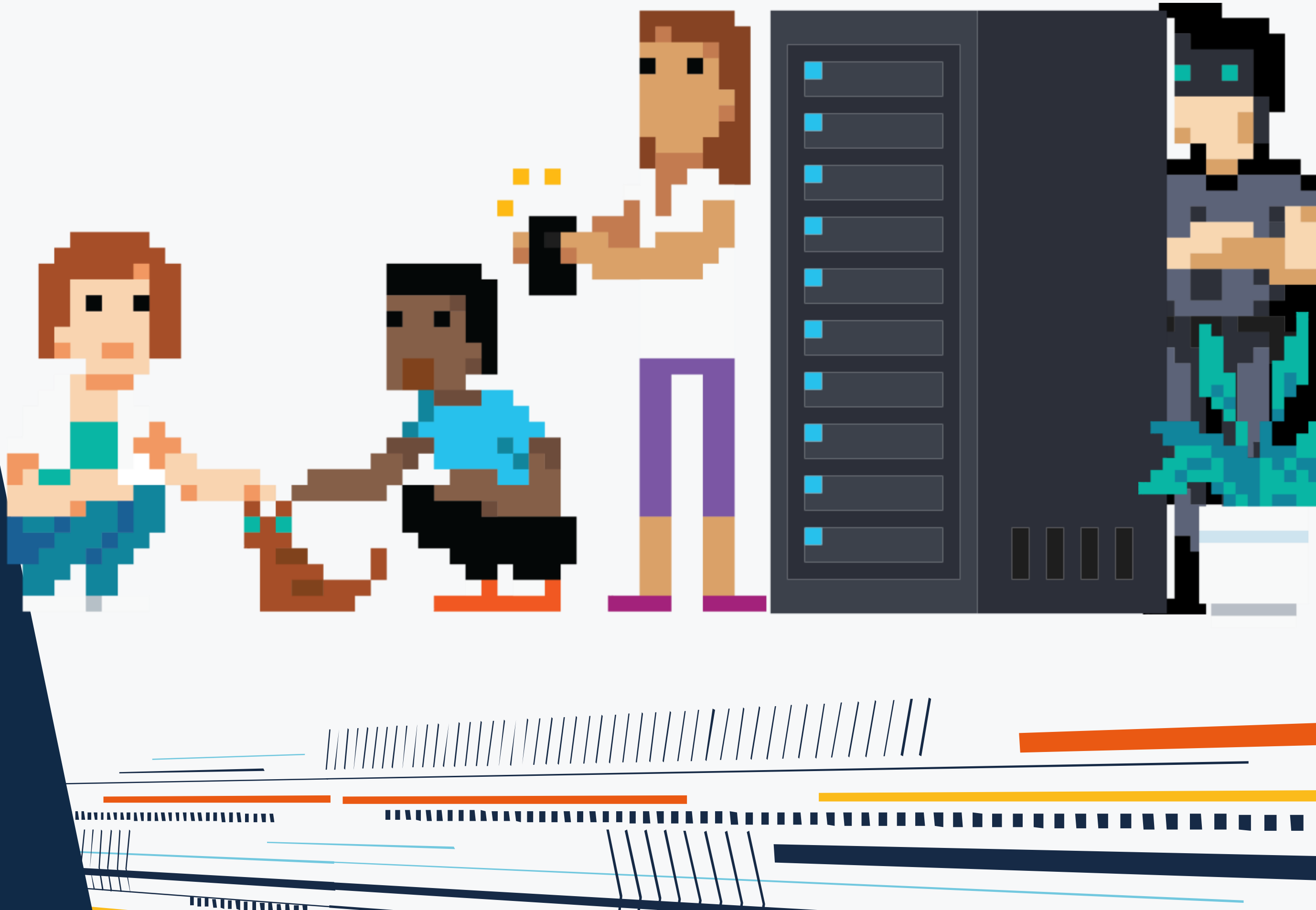
- Domain Admin, Enterprise Admin, and Schema Admin Group change monitoring
- Pass the hash, overpass the hash, and pass the ticket detection
- Detect the creation of a service on a domain controller
- Local Admin Group modified on member server
- Scheduled task creation
- Software was installed on a server
- Software was removed from a server
- System was powered off
- Kevin Holman’s failed RDP attempts monitor
- Loads more…

Demo

Sample configuration using GPO and default MP settings

For a full guide, checkout:

https://blogs.technet.microsoft.com/nathangau/2017/05/01/introducing-the-security-monitoring-management-pack-for-scom/



Alert Management process

Simply importing the MP and configuring auditing is not enough; someone must be responsible for responding to any alerts in a timely fashion

- Most rules are designed to allow the security team to respond quickly
- Normal business activities will generate alerts – these should be verified and not just closed (or alerts disabled)
- Document what is and is not being monitored, and why. Keep this up to date when SCOM tuning occurs.

https://blogs.technet.microsoft.com/nathangau/2016/02/04/the-anatomy-of-a-good-scom-alert-management-process-part-1-why-is-alert-management-necessary/

Recommendations

Enabling security auditing features across your estate can be challenging, so if you have limited resources these are our top 3 items

- Turn on Windows Event Forwarding in the desktop environment. Configure it to forward security and applocker logs to collector server(s)
- Turn on process auditing (4688 events)
- Turn on AppLocker in audit mode and configure for various commercially available tools (the most sophisticated attackers will not use these, but plenty of bad guys will).

Much of what this will detect are types of things that can normally happen, but now the security team has a means of verifying that the activities are legitimate and following proper business process/change management

Coffee Break: Resources

Let us know what you'd like us to cover:
squaredup.com/topics

See what's coming up next:
squaredup.com/coffee-break-series

Recordings and slides published via
squaredup.com/blog

YouTube playlist for series
https://www.youtube.com/playlist?list=PLJNXoi
GgmTEu3yZRGpPNWQbG9WMyihZFs

Follow up email, inc. resources, sent out after each webinar

Q&A

SquaredUp