THE CASE FOR BUILDING YOUR OWN SOC AUTOMATIONS

NATHANAEL KENYON
ABOUT ME

• 20 YEARS EXPERIENCE IN INFORMATION TECHNOLOGY WITHIN MILITARY, GOVERNMENT AND PRIVATE SECTORS

• MBA, CISSP, GXPN, GAWN, GMOB, GPYC, GNFA, GPEN, GCIA, GCIH, GCFE, GSEC, GCFA
ABOUT THE TOPIC

• **SOAR** was a popular topic at **SOC Summit 2018**
• **What can you do to automate?** Specific examples were hard to find.
• **Maybe my Google-FU is simply weak, but can an another example hurt?**
THE PURPOSE OF SOAR TOOLS

- Alleviate Staff shortages
- Reduce routine and burdensome work for analysts
- Reduce the number of tools an analyst has to interact with
- Improve Workflow management
HAS THIS EVER HAPPENED TO YOU?

• **Salesperson** “misrepresented product capabilities”
• **Tool changes** required you to make adjustments to your processes?
• **If this hasn’t happened to you yet, it probably will.**
WHY SHOULD YOU BUILD YOUR OWN SOC AUTOMATIONS?

• There is no magic product that will do everything for you

• The new security, automation, orchestration and response (SOAR) tools will not help you if you if you do not have your processes defined and the ability implement custom integrations. (Even if the salesperson says it will)

• Trying to do it yourself will tell you if you really need a new tool and give you valuable experience that will help you if you do purchase SOAR tools
PEOPLE, PROCESSES AND TECHNOLOGY

• Adequately trained staff will be more successful with lesser tools than poorly trained staff with best of breed, top of the line tools.

• There is an information security skills shortage in part because there are so many technologies that have to be secured.

• People bring skills, process is how you apply the skills, improving both of these is more important than acquiring new technology.
• Processes are ad hoc
• It is often a reactive and chaotic environment.

• Basic processes are in place.
• Still more of a reactive environment.

• Processes are well documented and implemented.

• The processes are evaluated based on the data that is collected.

• The environment has become proactive.
• Qualitative feedback allows for process improvement.
MAXIMIZING YOUR ANALYST

• Analysts should be investigating and mitigating threats
• Advanced analysts should be hunting for threats
• Make sure job tasks are appropriate for skill level
• Have analysts train and share knowledge with each other
SKILLS INVENTORY

• A human resource tool to help ensure that employees are a good fit for job/task needs

• Used to collect information about your analyst regarding their skills, abilities and experiences

• Include what skills/areas the analyst would like to improve in
“O” IS FOR ORCHESTRATION

- Orchestration – the organizing and coordination of workflow
- Establishing written procedures (Use Cases)
- Have your analyst write their individual use cases
- If capability degrades when any one person goes on leave, they need to write down what they are doing.
“A” is for Automation

- Automate all the things (That you can)
- Use automation for consistency and time savings
- There will always be a gap between what is available out of the box with your tools and what you will need
- Develop the skills within your team to write custom automations
GOAL: CREATE A TEST ENVIRONMENT TO PRACTICE SECURITY AUTOMATION

• Requirements: Python 2.7 with Juniper PY-EZ
• Virtual Box
• Vagrant
• Splunk Enterprise with Trial or Development License
**STEPS**

- [HTTPS://GITHUB.COM/JUNIPER/vqfx10k-vagrant](https://github.com/Juniper/vqfx10k-vagrant) - Use one of the full versions
- **Vagrant up** – This will download the virtual images and run them in Virtual Box
- This take a **LONG TIME** to boot up, but you will have a functional vQFX switch.
- **Pip install junos-eznc** – This will install all the dependencies for using python to change configurations on JUNOS Devices (MX,QFX,SRX)
- **Install Splunk Enterprise**
{master:0}[edit]
root@vqfx-re# show forwarding-options analyzer portmirror {
    input {
        ingress {
            interface xe-0/0/0.0;
        }
    }
}
output {
    interface xe-0/0/1.0;
}

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Link</th>
<th>Proto</th>
<th>Local</th>
</tr>
</thead>
<tbody>
<tr>
<td>gr-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pfe-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pfe-0/0/0.16383</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td></td>
</tr>
<tr>
<td>pfh-0/0/0</td>
<td>up</td>
<td>up</td>
<td>inet6</td>
<td></td>
</tr>
<tr>
<td>pfh-0/0/0.16383</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td></td>
</tr>
<tr>
<td>pfh-0/0/0.16384</td>
<td>up</td>
<td>up</td>
<td>inet</td>
<td></td>
</tr>
<tr>
<td>xe-0/0/0</td>
<td>up</td>
<td>up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-0/0/0.0</td>
<td>up</td>
<td>up</td>
<td>eth-switch</td>
<td></td>
</tr>
<tr>
<td>xe-0/0/1</td>
<td>down</td>
<td>down</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xe-0/0/1.0</td>
<td>up</td>
<td>down</td>
<td>eth-switch</td>
<td></td>
</tr>
</tbody>
</table>
Edit Alert

Search: source="C:\Windows\System32\winevt\Logs\Windows PowerShell.evtx"

Alert type: Scheduled, Real-time

Trigger Conditions
Trigger alert when: Per-Result
Throttle: off

Trigger Actions
When triggered: Run a script

⚠️ The run a script alert action is officially deprecated. Create a custom alert action to package a custom script instead. Learn more

File name: pytest.py
Located in $SPLUNK_HOME/bin/scripts or $SPLUNK_HOME/etc/search/bin/scripts
# $SPLUNK_HOME/bin/scripts/pytest.py

from jnpr.junos import Device
from jnpr.junos.utils.config import Config

dev = Device(host='192.168.56.101', user='pyuser', password='Password')
dev.open()

cu = Config(dev)

config_set = """delete interfaces xe-0/0/1 disable"""
cu.load(config_set, merge=True)
cu.commit()

dev.close()
MAXIMIZING YOUR CURRENT TOOL SET

- **Too many tools is a problem**
- **Implement all the features of the tools you have before you add more tools.**
- **Maximize by minimizing**
PURCHASE CONSIDERATIONS

• Are you getting full value from the tools you currently have?
• Do your analysts have the time to learn another tool or process?
• Is it possible that acquiring a new tool could make things worse?
FINAL THOUGHTS

• **Utilize your analysts to help develop your orchestration and automation procedures**

• **Maximize the current tools that are already in your SOC before adding more tools**

• **Upgrade your skills inventory**
RESOURCES

https://www.vagrantup.com/

https://www.virtualbox.org/

https://github.com/Juniper/py-junos-eznc

https://github.com/Juniper/vqfx10k-vagrant

https://www.python.org/