




# Cybersecurity Automation

---

Eliminating noise, making life easier,  
and doing more with less



# Agenda

---

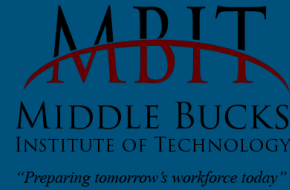
- About Me
- Cybersecurity Automation Overview
- Tools
- Use Cases
- Learning More

The secret word is...

**Banana**

# About Me

- Senior Cybersecurity Engineer @ Zoox
- New to Roanoke, VA
- 14 years in career
- MS Data Analytics (WGU)
- BS Security and Risk Analysis (PSU)



# Cybersecurity Automation

---

- Using scripts and 3rd party tools to complete cybersecurity tasks
- Faster (but takes time to build)
- More accurate (must be peer reviewed)
- Does not replace the need for analysts (but does reduce the number we need)

# Tools

---

- Scripting languages (go, Python, PowerShell)
- SOAR Platforms (Cortex XSOAR, Splunk Phantom, TheHive)
- Data analytics tools (Jupyter, R)

# Common Use Cases

---

# Phishing Analysis

---

## The Old Way

- Analysts triage emails in an inbox
- Manual lookup of URLs, sender domain, etc.
- Risk of accidentally clicking on malicious links
- Suspicious attachments downloaded to analyst workstation
- Each analyst does their own thing

## With Automation

- Automated lookups
- Screenshots of URLs
- Automated checks for SPF, DMARC, DKIM
- Attachments are analyzed automatically
- Correlation across multiple investigations
- Repeatable processes
- ML models

# Employee Onboarding and Offboarding

---

## The old way

- HR sends an email or files a ticket with IT
- User accounts are created/disabled manually
- Permissions and licenses are added/removed manually

## With Automation

- HR sends an email or files a ticket with IT
- A script creates the new account automatically
- Based on the user's role, permissions and licenses are added/removed automatically
- Offboarding - remove rights to sensitive files as soon as notice is given



# Asset Database / Tool Coverage

---

- Most security teams have a handful of tools
- How do we ensure all of our (applicable) devices are on all our tools?
- Excel/Google Sheets works but it takes a lot of time...every time...
- We can use Python to analyze this data and identify the coverage gaps

# Metrics

---

- Most vendors provide out of the box metrics, but leadership often wants something specific
- Rather than making pivot tables and doing vlookups in excel, practitioners write scripts to process data and enrich it from other sources

# Wrap-Up



# Challenges

---

## Requirements

- Good tools
- Well-defined processes
- Time
- Skills

## Other Challenges

- Distrust of robots
- Job security
- Budget constraints

# This is cool...how do I get started?

---

- iPhone users - Apple Shortcuts
- Homelab
  - MISP
  - TheHive
- Data analytics python libraries
  - sklearn
  - pandas
- Other home projects

**DISCLAIMER: Web scraping can get you banned from a site, and never try to probe systems you don't own!**

# Resources

---

- Threat Hunting Jupyter Notebooks - <https://github.com/OTRF/ThreatHunter-Playbook>
- Automate The Boring Stuff - <https://automatetheboringstuff.com/>
- Apple Shortcuts - <https://www.reddit.com/r/shortcuts/>
- TheHive Training VM - <https://strangebee.com/thehive-virtual-machine/>

# Questions?

