A Threat Hunting Walkthrough

Lauren Proehl

Marsh McLennan

Lauren Proehl

Sr Manager, Global Cyber Defense

- Eight years in security
- Three years in telecommunications industry
- Led SOC, IR, Threat Hunt, CTI, and automation efforts
- SecKC, BSides KC CFP, MSU Advisory Board
    - Trying to escape computers by running in the woods

A human-driven
process to identify artifacts associated with
a ***previously undetected*** *intrusion or breach that was*
not identified by existing security controls.

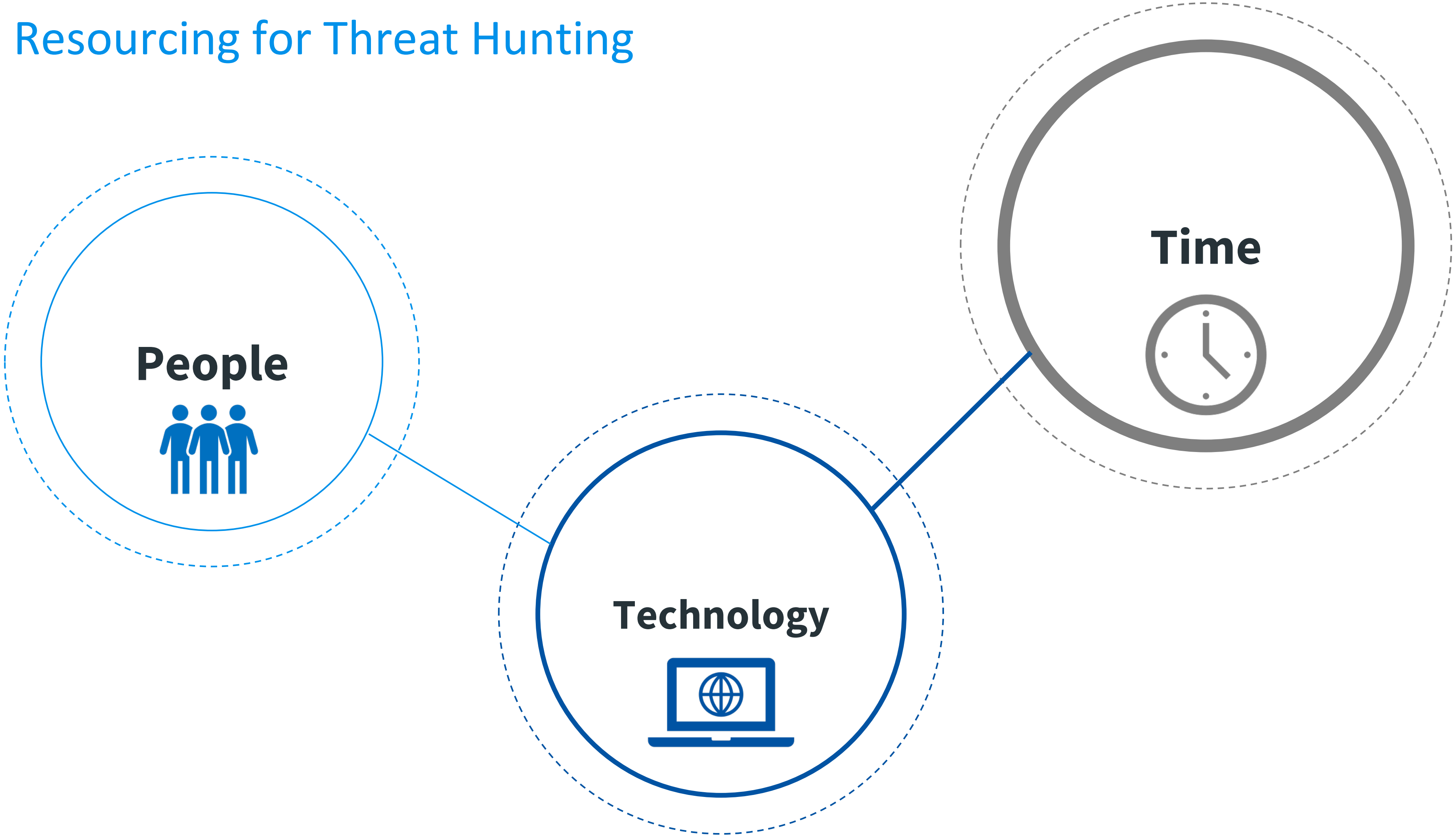
What is threat hunting?

- Process driven iterative work
- Hypothesis driven
- Proactive
- Behavior and/or pattern focused

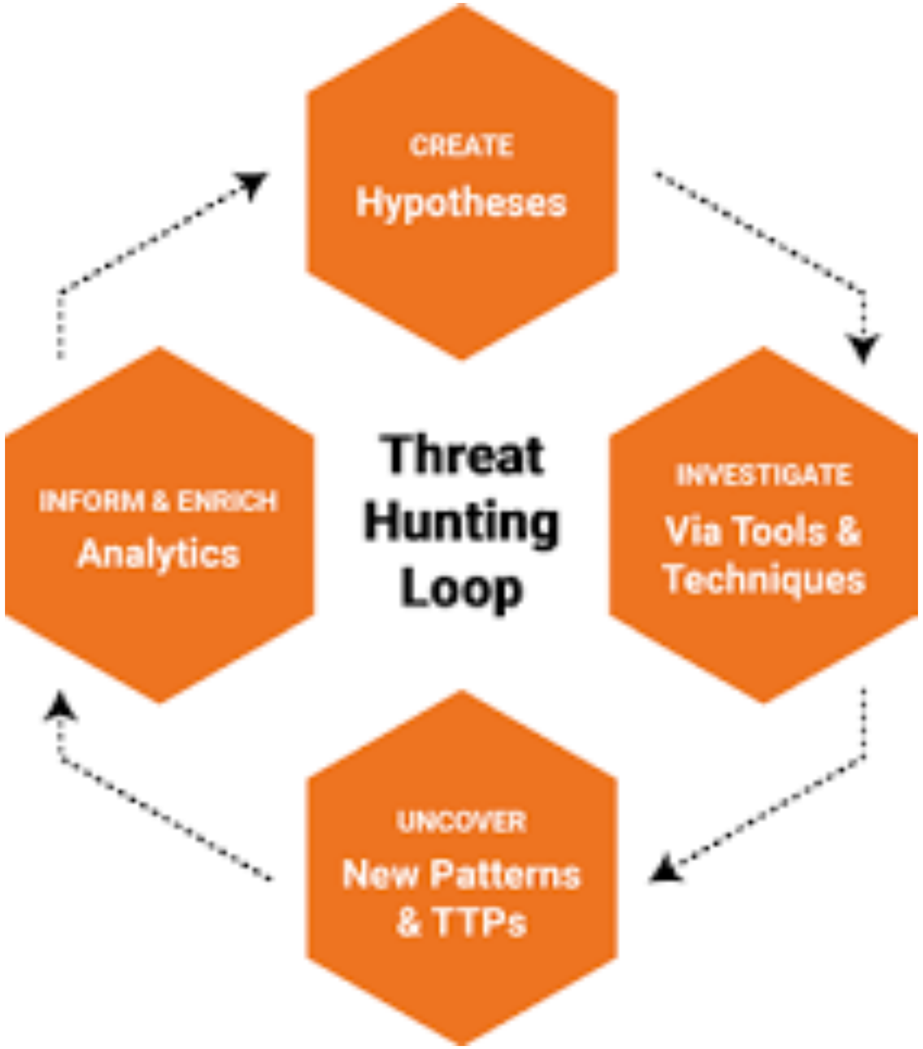
What isn’t threat hunting?

- Looking up IOC matches
- Looking through existing detections
- Singular exercise without a process

Resourcing for Threat Hunting



Threat Hunting Process



A Case for Emulation

- There should always be something to find
- Ripping queries off the Internet doesn’t always yield something
- Two for one exercise
- Frequently finds control gaps in addition to unidentified malicious activity

Build Better Hypotheses

- Bad inputs mean bad outputs

- Too much freedom = bad
- Too little freedom = bad

- Five elements of a good hypothesis:
  - Relevancy
  - Target
  - Technique
  - Payload/Action on Objectives
  - Attacker Type (optional)

Good Hypothesis

PowerShell is being leveraged on endpoints to execute malware in memory

Better Hypothesis

Attackers are compiling exploits locally on servers/clients to use, and using basic naming schema, like “exploit.exe.”

Best Hypothesis

WSL (the Windows Unix Subsystem) is being used for malicious scripting purposes and cross compatibility malware execution by malicious insiders.

Types of Threat Hunting

Searching

Querying data for specific findings

Clustering

Statical technique of separating groups of data points

Grouping

Taking multiple unique artifacts and identifying overlaps

Stack Counting

Counting several occurrences and analyzing outliers

Hunt What Matters

Industry

The type of business you do, the customers your serve, the suppliers you rely on

Geolocation

Global, national, regional

Technology Stack

What make your business go

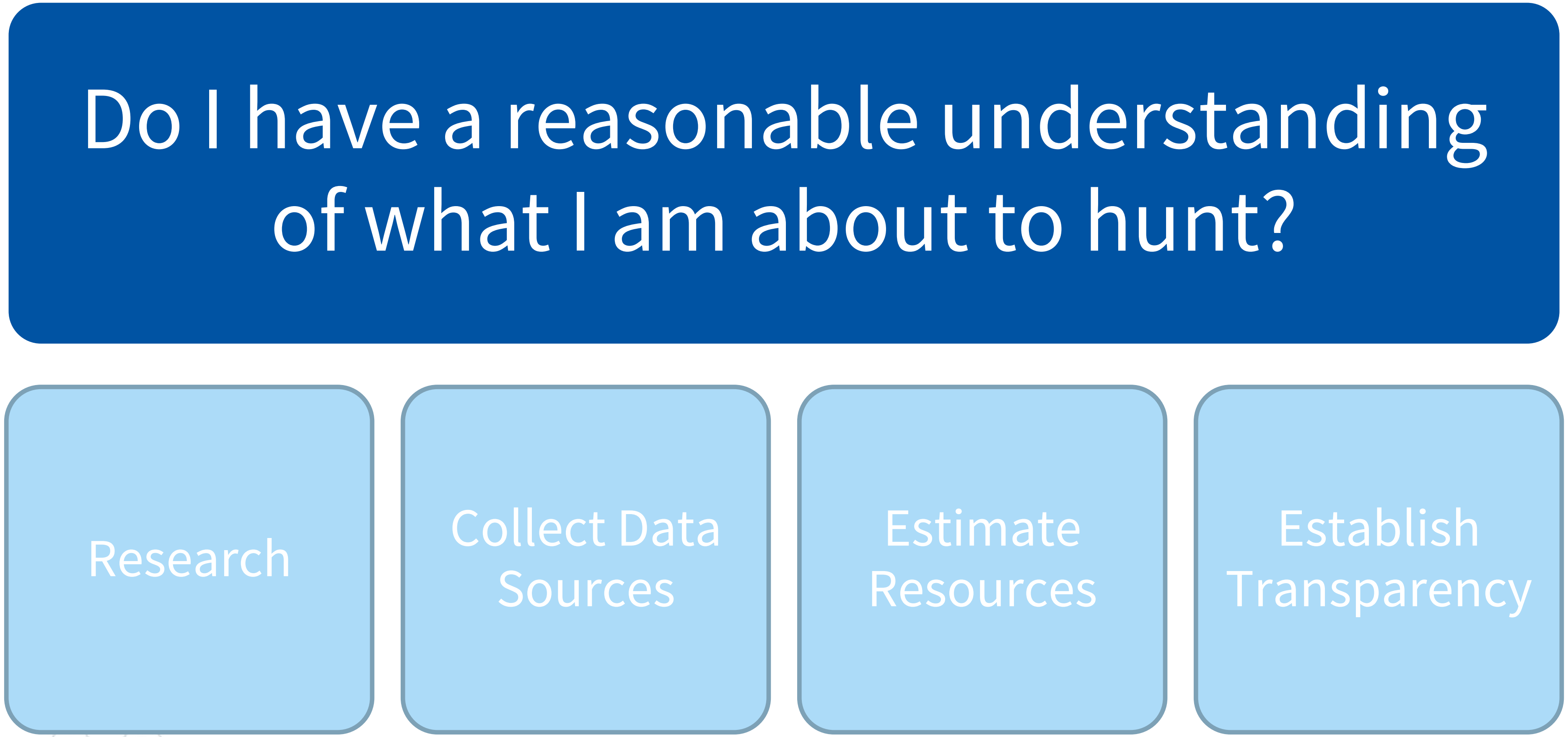
Crown Jewels

Very important people, assets, applications, or processes

Trends

What you are seeing from a detection and response perspective

Pre-Hunt Preparation



Do I have a reasonable understanding of what I am about to hunt?

Research

Collect Data Sources

Estimate Resources

Establish Transparency

Real World Hunt + Process

- Hypothesis: Company employees are sending company confidential data to private email addresses as a way to exfiltrate data for a potential new job.

- Data Sources: Email, firewall, web proxy, endpoint (optional)

- Things to look for:
  1. Emails outbound to Gmail, Yahoo, Hotmail, AOL, or iCloud addresses
  2. Web access to private email portals
  3. Large uploads of files to cloud hosting websites
  4. Zipping of entire folders on host

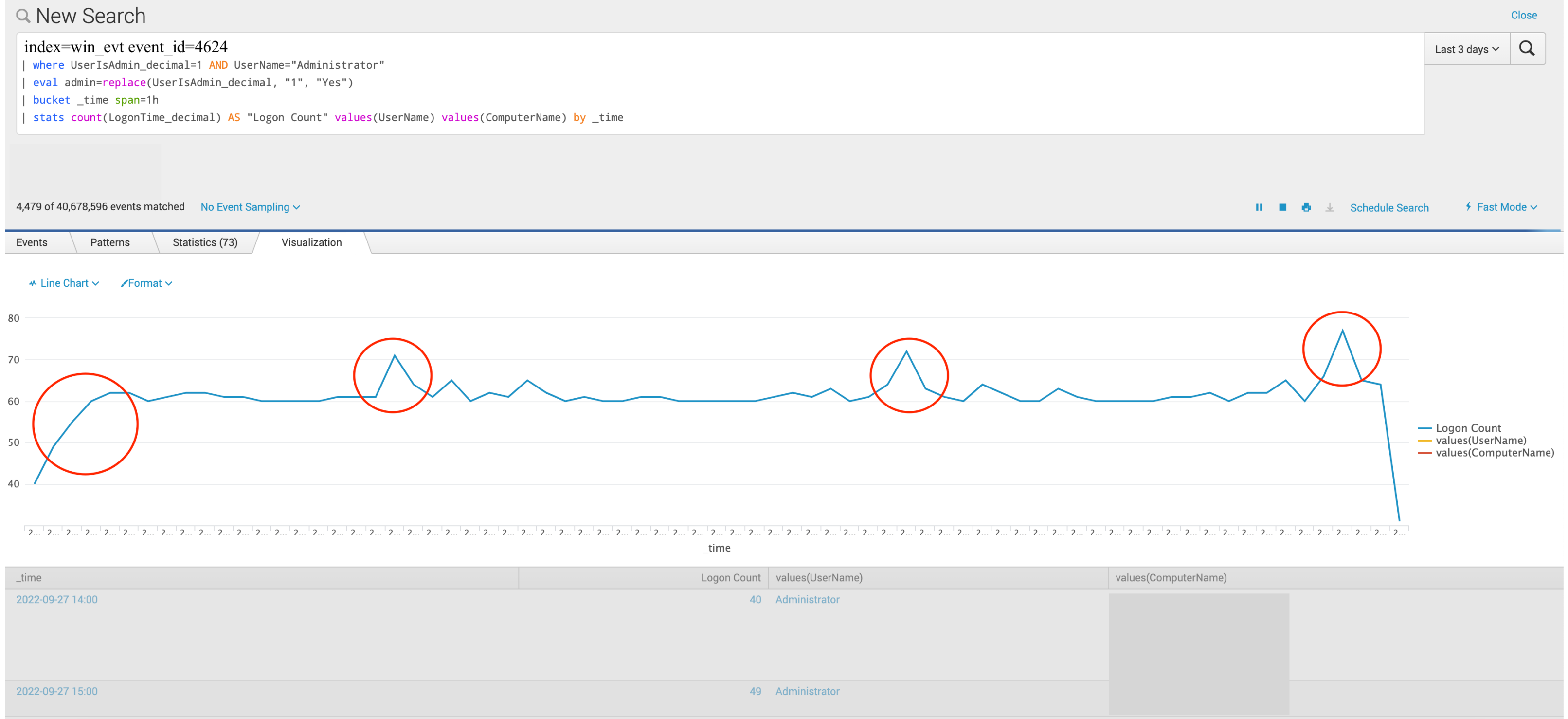
- Pseudo queries:
  - Log_type=email AND sender.address=lauren.Proehl@mmc.com AND receiver.address CONTAINS “gmail.com”
  - (Log_type=proxy OR log_type=firewall) AND (domain=“gmail.com” OR domain=“mail.google.com”) AND username=”lauren”
  - (Log_type=proxy OR log_type=firewall) AND (domain=“gmail.com” OR domain=“mail.google.com”) AND username=”lauren” AND upload_bytes >= 26214400
  - (Log_type=proxy OR log_type=firewall) AND (domain CONTAINS ”upload” OR request_method=“PUT”) AND username=”lauren”
  - Log_type=endpoint AND event_type=”file_create” AND file_name=“*.zip”

- MITRE Techniques: T1560 (Archive Collected Data), T1567 (Exfiltration Over Web Service), T1567.002 (Exfiltration To Cloud Storage)

- How to not hunt this again:
  1. Block access to personal email accounts
  2. Block email forwarding rules
  3. Block access to personal cloud services if applicable
  4. Weekly report of attempts to access personal email services
  5. Weekly report of emails sent to personal email services with large attachments

Local administrator account creation or compromise

- Look for unknown or new local administrator accounts
- Logon times for local administrator accounts
- Stack to find non-standard times to determine compromise



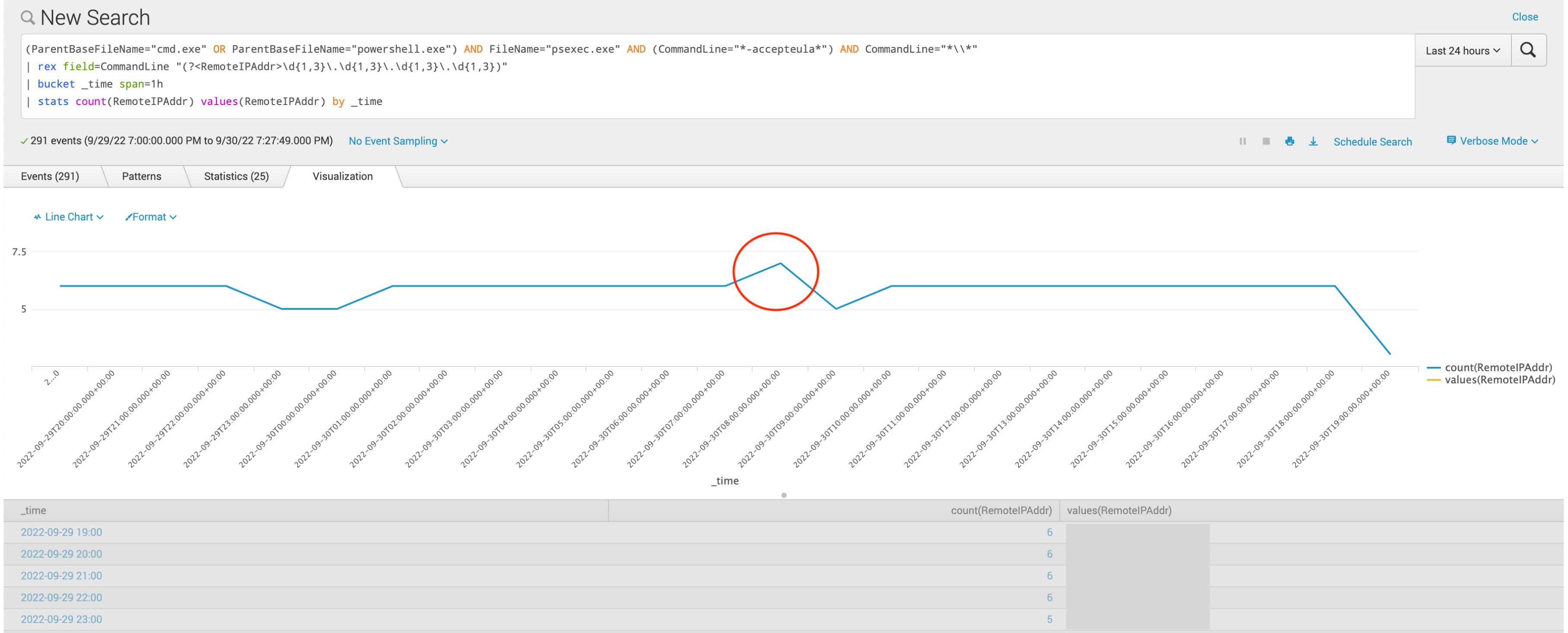
```
index=win_evt event_id=4624
| where UserIsAdmin_decimal=1 AND UserName="Administrator"
| eval admin=replace(UserIsAdmin_decimal, "1", "Yes")
| bucket _time span=1h
| stats count(LogonTime_decimal) AS "Logon Count" values(UserName) values(ComputerName) by _time
```

4,479 of 40,678,596 events matched

_time	Logon Count	values(UserName)	values(ComputerName)
2022-09-27 14:00	40	Administrator	[redacted]
2022-09-27 15:00	49	Administrator	

Suspicious remote psexec attempts

- Often used for lateral movement
- Look for weird remote addresses or large variance in remote addresses from same source
- Look for odd times of psexec usage to remote addresses



New Search

Close

```
(ParentBaseFileName="cmd.exe" OR ParentBaseFileName="powershell.exe") AND FileName="psexec.exe" AND (CommandLine="*-accepteula*") AND CommandLine="*\\*"
| rex field=CommandLine "(?<RemoteIPAddr>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"
| bucket _time span=1h
| stats count(RemoteIPAddr) values(RemoteIPAddr) by _time
```

Last 24 hours

✓ 291 events (9/29/22 7:00:00.000 PM to 9/30/22 7:27:49.000 PM)

No Event Sampling

Schedule Search

Verbose Mode

Events (291) | Patterns | Statistics (25) | Visualization

Line Chart

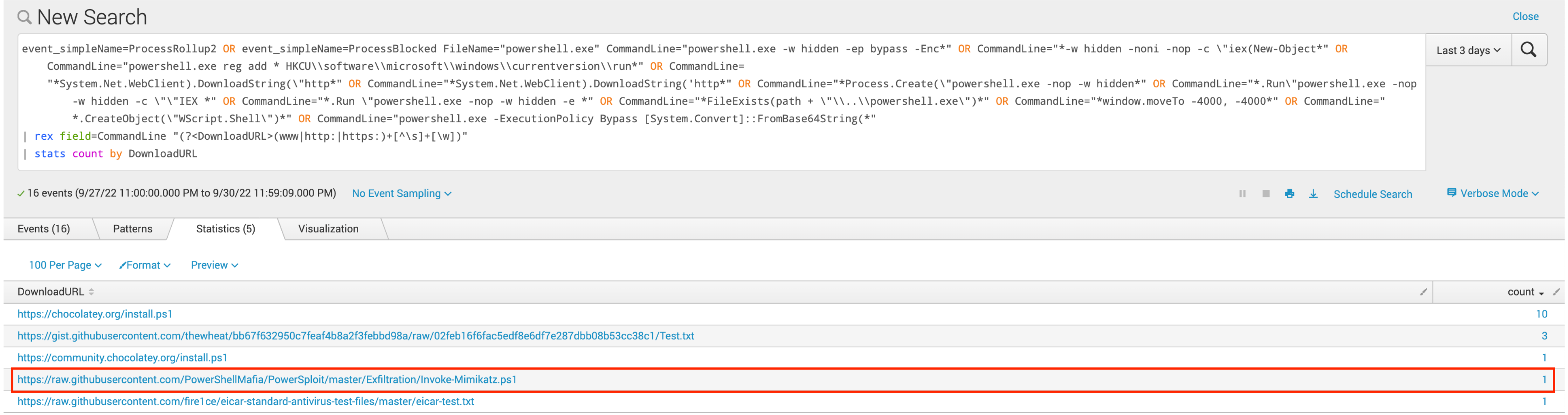
Format

7.5
5
2...0
2022-09-29T20:00:00.000+00:00
2022-09-29T21:00:00.000+00:00
2022-09-29T22:00:00.000+00:00
2022-09-29T23:00:00.000+00:00
2022-09-30T00:00:00.000+00:00
2022-09-30T01:00:00.000+00:00
2022-09-30T02:00:00.000+00:00
2022-09-30T03:00:00.000+00:00
2022-09-30T04:00:00.000+00:00
2022-09-30T05:00:00.000+00:00
2022-09-30T06:00:00.000+00:00
2022-09-30T07:00:00.000+00:00
2022-09-30T08:00:00.000+00:00
2022-09-30T09:00:00.000+00:00
2022-09-30T10:00:00.000+00:00
2022-09-30T11:00:00.000+00:00
2022-09-30T12:00:00.000+00:00
2022-09-30T13:00:00.000+00:00
2022-09-30T14:00:00.000+00:00
2022-09-30T15:00:00.000+00:00
2022-09-30T16:00:00.000+00:00
2022-09-30T17:00:00.000+00:00
2022-09-30T18:00:00.000+00:00
2022-09-30T19:00:00.000+00:00
_time
count(RemoteIPAddr)
values(RemoteIPAddr)

_time	count(RemoteIPAddr)	values(RemoteIPAddr)
2022-09-29 19:00	6	
2022-09-29 20:00	6	
2022-09-29 21:00	6	
2022-09-29 22:00	6	
2022-09-29 23:00	5	

Downloads from the internet via PowerShell

- Privilege escalation, lateral movement, collection, exfiltration
- Look for websites you don’t recognize – Github is a risk!
- Make sure you have defense in depth



```
event_simpleName=ProcessRollup2 OR event_simpleName=ProcessBlocked FileName="powershell.exe" CommandLine="powershell.exe -w hidden -ep bypass -Enc*" OR CommandLine="*-w hidden -noni -nop -c \"iex(New-Object*" OR
    CommandLine="powershell.exe reg add * HKCU\\software\\microsoft\\windows\\currentversion\\run*" OR CommandLine=
    "*System.Net.WebClient).DownloadString(\"http*" OR CommandLine="*System.Net.WebClient).DownloadString('http*" OR CommandLine="*Process.Create(\"powershell.exe -nop -w hidden*" OR CommandLine="*.Run\"powershell.exe -nop
        -w hidden -c \"\"IEX *" OR CommandLine="*.Run \"powershell.exe -nop -w hidden -e *" OR CommandLine="*FileExists(path + \"\\..\\powershell.exe\")*" OR CommandLine="*window.moveTo -4000, -4000*" OR CommandLine="
        *.CreateObject(\"WScript.Shell\")*" OR CommandLine="powershell.exe -ExecutionPolicy Bypass [System.Convert]::FromBase64String(*"
| rex field=CommandLine "(?<DownloadURL>(www|http:|https:)+[^\s]+[\w])"
| stats count by DownloadURL
```

✓ 16 events (9/27/22 11:00:00.000 PM to 9/30/22 11:59:09.000 PM)

DownloadURL	count
https://chocolatey.org/install.ps1	10
https://gist.githubusercontent.com/thewheat/bb67f632950c7feaf4b8a2f3febbd98a/raw/02feb16f6fac5edf8e6df7e287dbb08b53cc38c1/Test.txt	3
https://community.chocolatey.org/install.ps1	1
https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1	1
https://raw.githubusercontent.com/fire1ce/eicar-standard-antivirus-test-files/master/eicar-test.txt	1

Other Hunt Ideas

- **Exfiltration:** Employees have committed sensitive information, including API keys, to public code repositories or forums and put internal data at risk
- **Defense Evasion:** Attackers have disabled Windows Defender, Windows Firewall, and cleared Windows Events to avoid detection
- **Privilege Escalation:** Employees are practicing hacking activities and/or researching hacking methods on enterprise networks
- **Impact:** Managed hosts have been infected with ransomware and have not alerted through existing security detections due to new decryption notification files in use.
- **Initial Access:** Attackers are using simple, text-only emails to avoid setting off detection signatures and social engineer finance or HR employees
- **Lateral Movement:** Attackers are attempting to compromise third-party vendors in order to gain a foothold in your enterprise network
- **Execution:** OS X endpoints may be targeted for attacks due to their high-level users and differing security controls. Attacks that no longer easily work on Windows could work on Macs.

Other Hunt Content

MITRE ATT&CK™

The ThreatHunting Project

ThreatHunting

Open Threat Research

THREAT HUNTER Playbook

Thank you!

https://github.com/triw0lf/NTCA-Cybershare-22

https://laurenproehl.com

https://twitter.com/jotunvillur