## Supercharge your SOC with 3 Killer Threat Hunting Use Cases

Patrick Keenan, Principal Security Engineer



### INTRODUCTIONS



Patrick Keenan
Senior Security Engineer
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

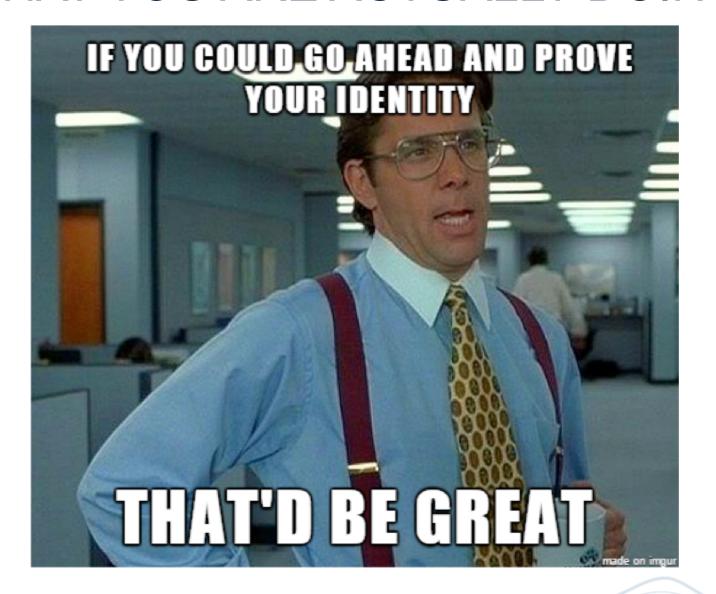


### WHAT YOU THOUGHT YOU WOULD BE DOING





### 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 users 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

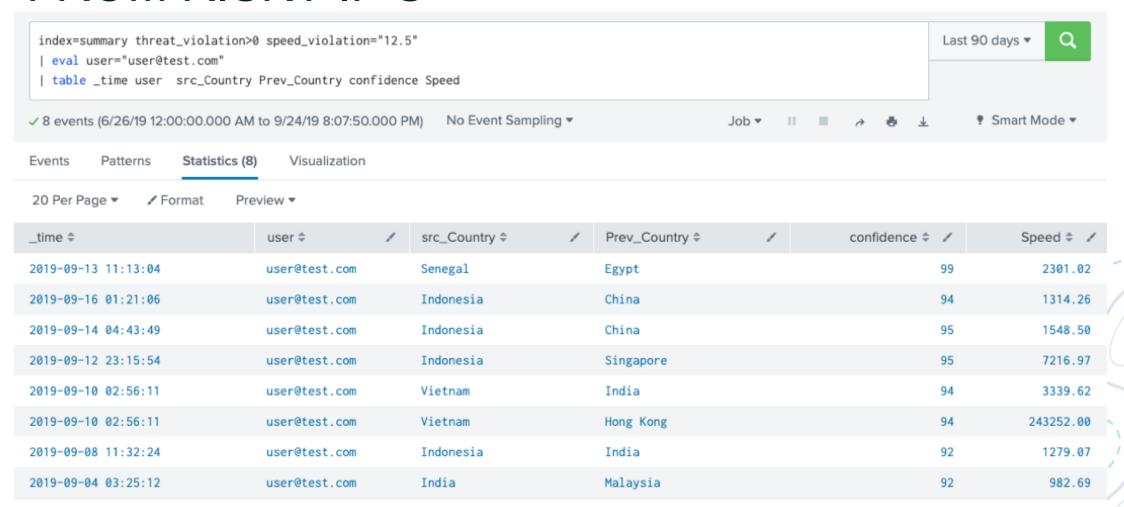


### RISK MODELING – RISKY COUNTRIES

Events Patterns Statistics (1,703) Visualization	<pre>index=summary blacklisted_src_Country_violation&gt;0 countr   eval user="user@test.com"   table _time user src_Country</pre>	ry_anomaly>0	Last 7 days ▼ Q
20 Per Page ▼	✓ 1,703 events (9/17/19 8:00:00.000 PM to 9/24/19 8:02:30.000 P	M) No Event Sampling ▼	Job ▼ II ■ → 🖶 🖳 § Smart Mode ▼
time \$	Events Patterns Statistics (1,703) Visualization		
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	20 Per Page ▼		< Prev 1 2 3 4 5 6 7 8 Next >
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	_time	user \$	<pre> ✓ src_Country    </pre>
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 15:31:16	user@test.com	Turkey
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 15:44:09	user@test.com	Turkey
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 13:53:48	user@test.com	Nigeria
2019-09-24 15:20:39	2019-09-24 14:07:31	user@test.com	Nigeria
2019-09-24 15:20:32 user@test.com Russia	2019-09-24 14:44:50	user@test.com	South Africa
	2019-09-24 15:20:39	user@test.com	Russia
2019-09-24 15:18:44 user@test.com Russia	2019-09-24 15:20:32	user@test.com	Russia
	2019-09-24 15:18:44	user@test.com	Russia

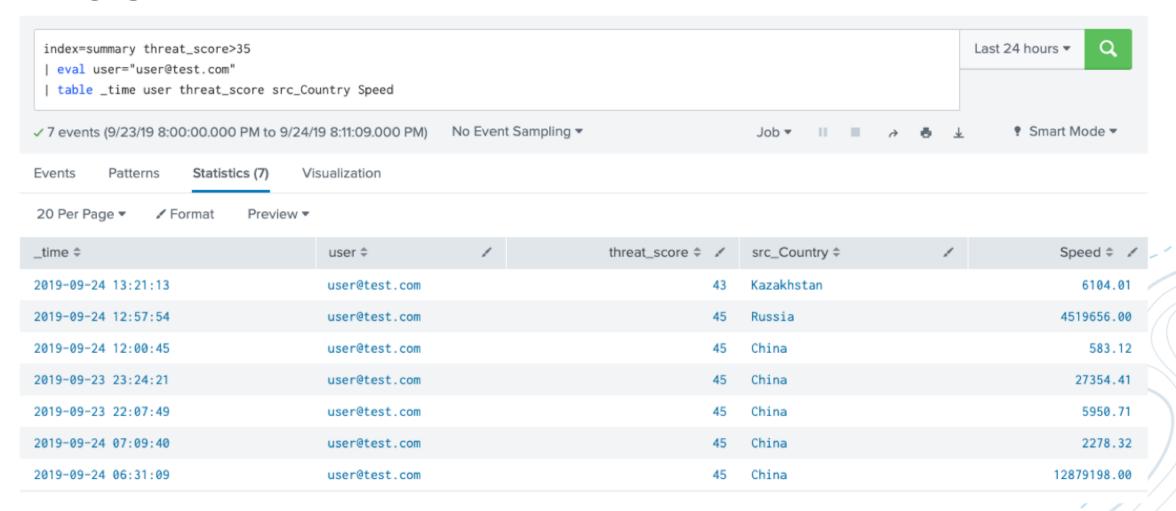


## RISK MODELING – SPEED VIOLATIONS FROM RISKY IP'S





## RISK MODELING – PUTTING IT ALL TOGETHER





# 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.



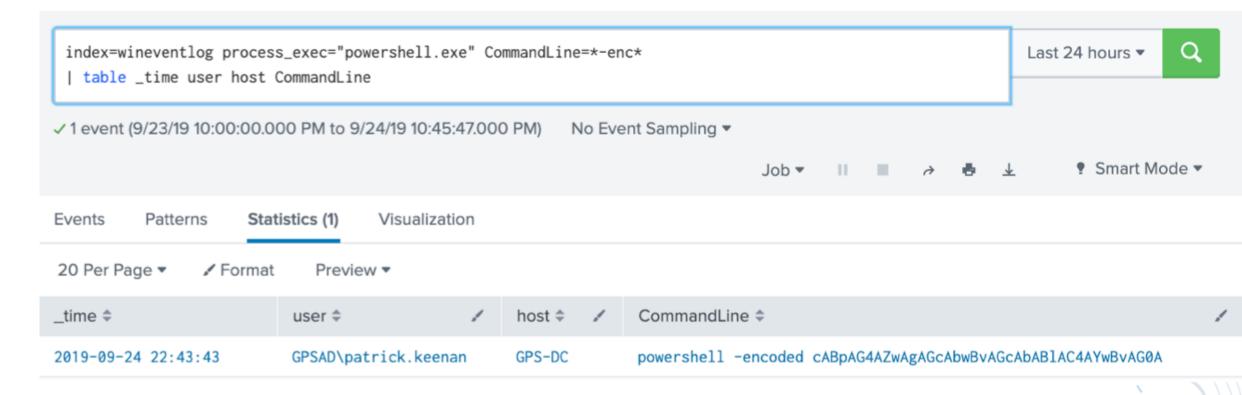
#### POWERSHELL HUNTING

#### 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





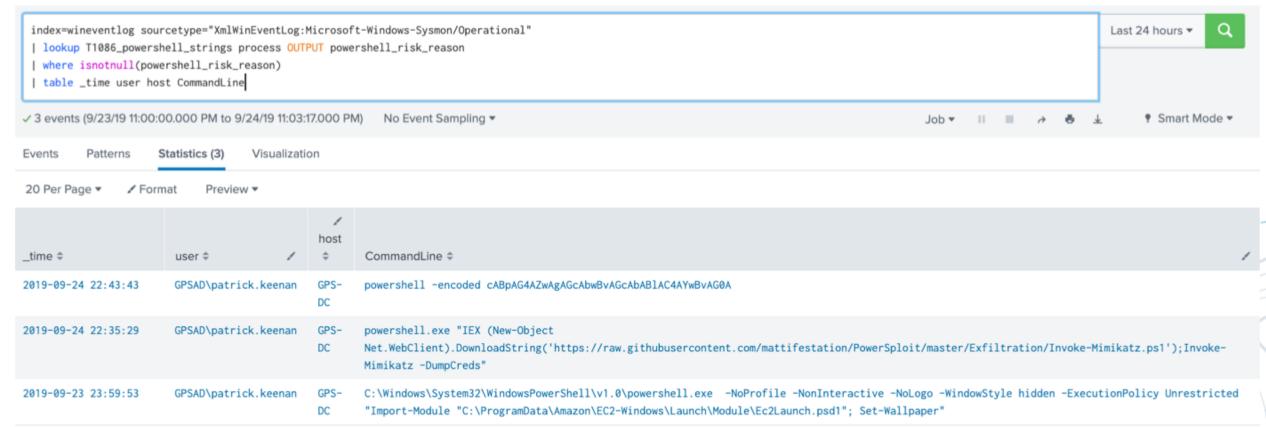
19

## 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





## 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



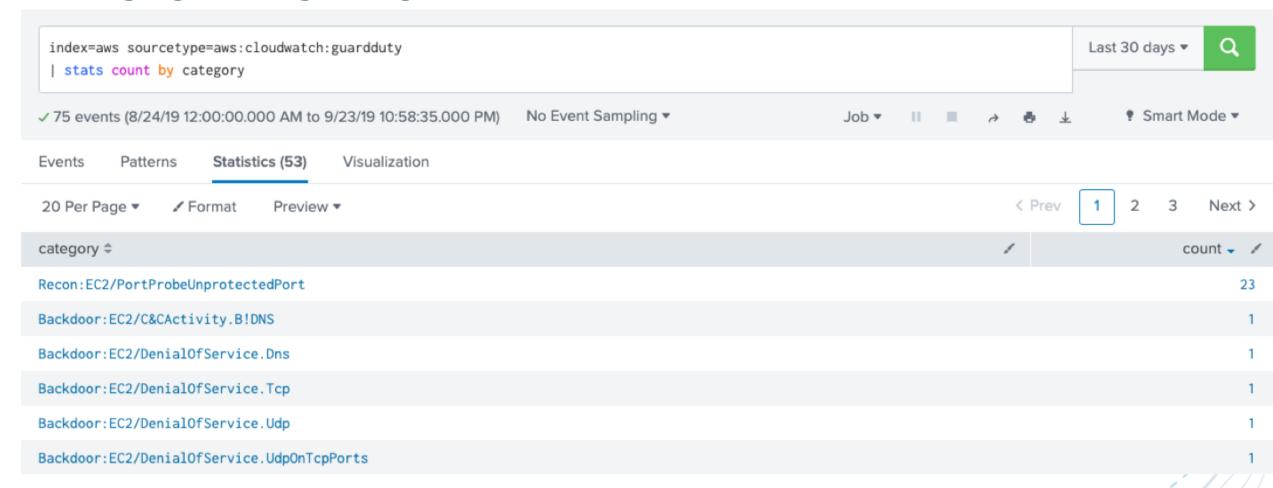
#### SEARCHING - AWS GUARD DUTY

Last 30 days ▼ a 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 √ 4 events (8/25/19 12:00:00.000 AM to 9/24/19 11:29:22.000 PM) No Event Sampling ▼ ¶ Smart Mode ▼ Job ▼ Statistics (4) Events Patterns Visualization 20 Per Page ▼ ✓ Format Preview ▼ severity \_time 🕏 action \$ category \$ signature \$ UnauthorizedAccess: IAMUser/InstanceCredentialExfiltration 2019-09-18 critical allowed Credentials for instance role GeneratedFindingUserName used from external IP 20:11:03.925 address. UnauthorizedAccess: EC2/RDPBruteForce 198.51.100.0 is performing RDP brute force 2019-09-18 low allowed attacks against i-99999999. 20:11:03.802 UnauthorizedAccess: EC2/SSHBruteForce 198.51.100.0 is performing SSH brute force 2019-09-18 low allowed attacks against i-99999999. 20:11:14.146 2019-09-18 UnauthorizedAccess: IAMUser/ConsoleLogin Unusual console login was seen for principal medium allowed GeneratedFindingUserName. 20:11:10.093



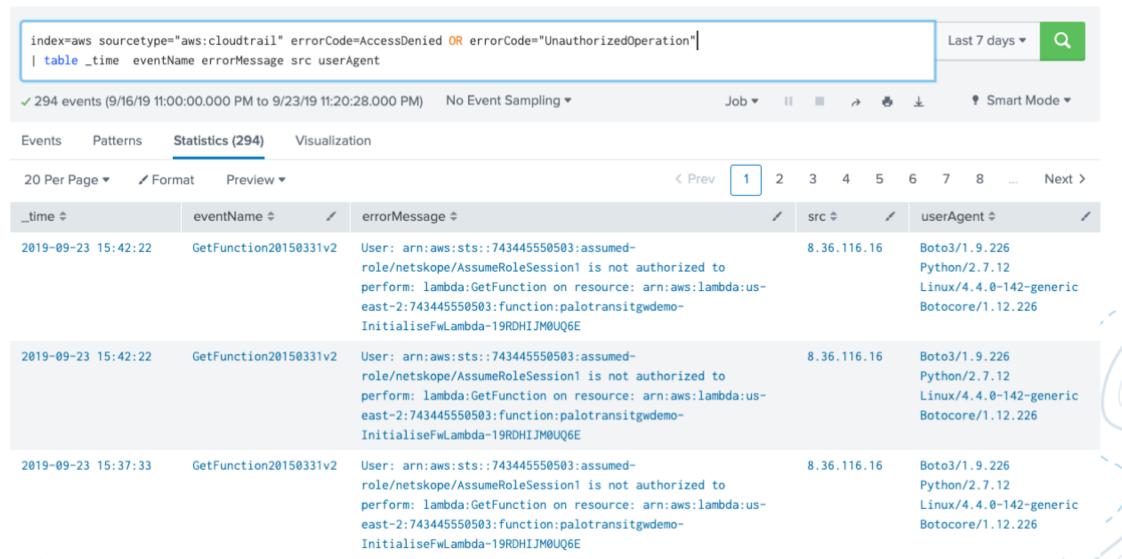
25

## STACK COUNTING – AWS GUARD DUTY SIGNATURES





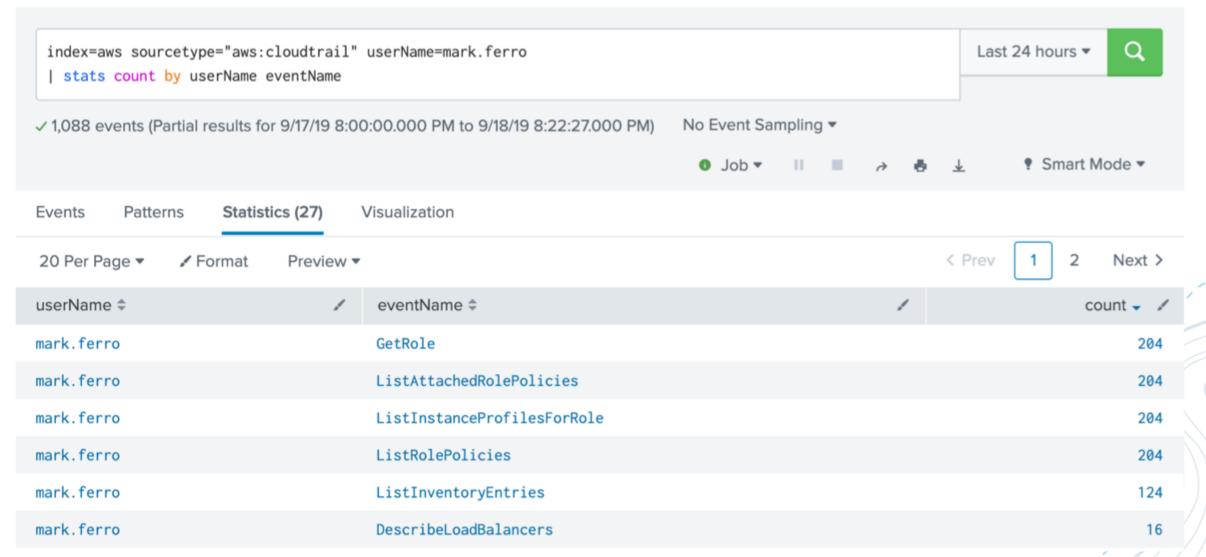
### SEARCHING - UNAUTHORIZED API CALLS





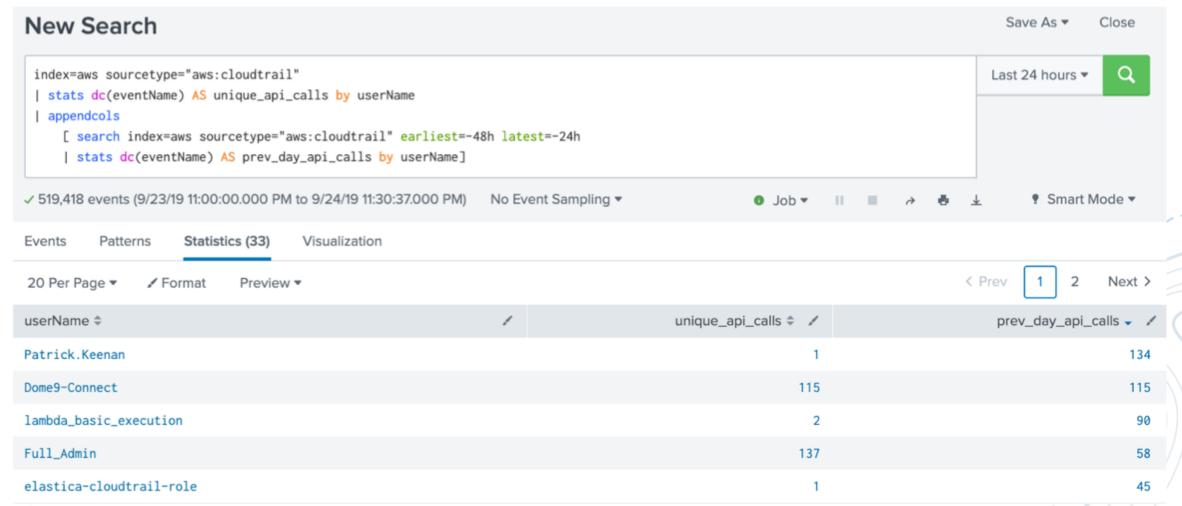
27

### STACK COUNTING - API CALLS



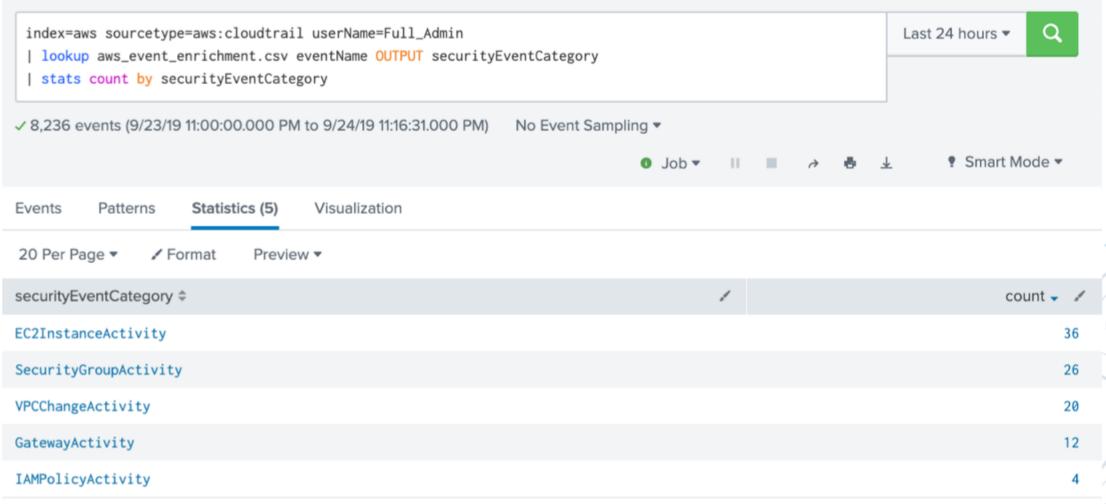


## STACK COUNTING – UNIQUE API CALLS OVER TIME



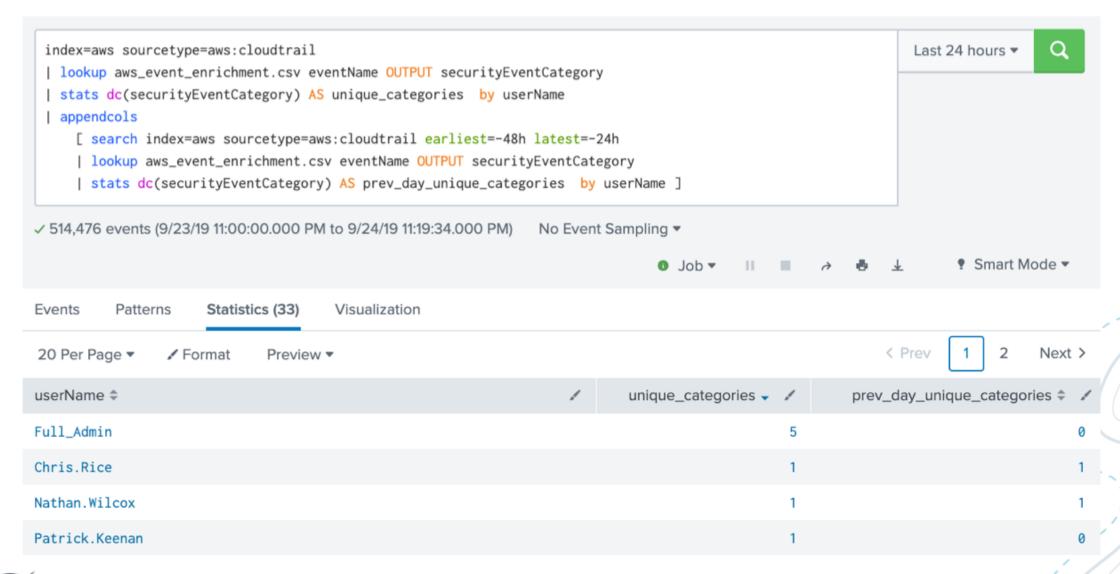


## STACK COUNTING/ENRICHMENT – API CATEGORIES





### USER ACTIONS – THE KITCHEN SINK





## Thank You

Patrick Keenan, GuidePoint Security GuidePointSecurity.com

