.conf18

splunk>

An Introduction to Fraud Detection with Splunk

How Sony Interactive Entertainment uses Splunk for Fraud Prevention

Grant Walthall – Security Engineer @ SIE

Beau Morgan – Staff SE @ Splunk

August 2018 | Version 1.0

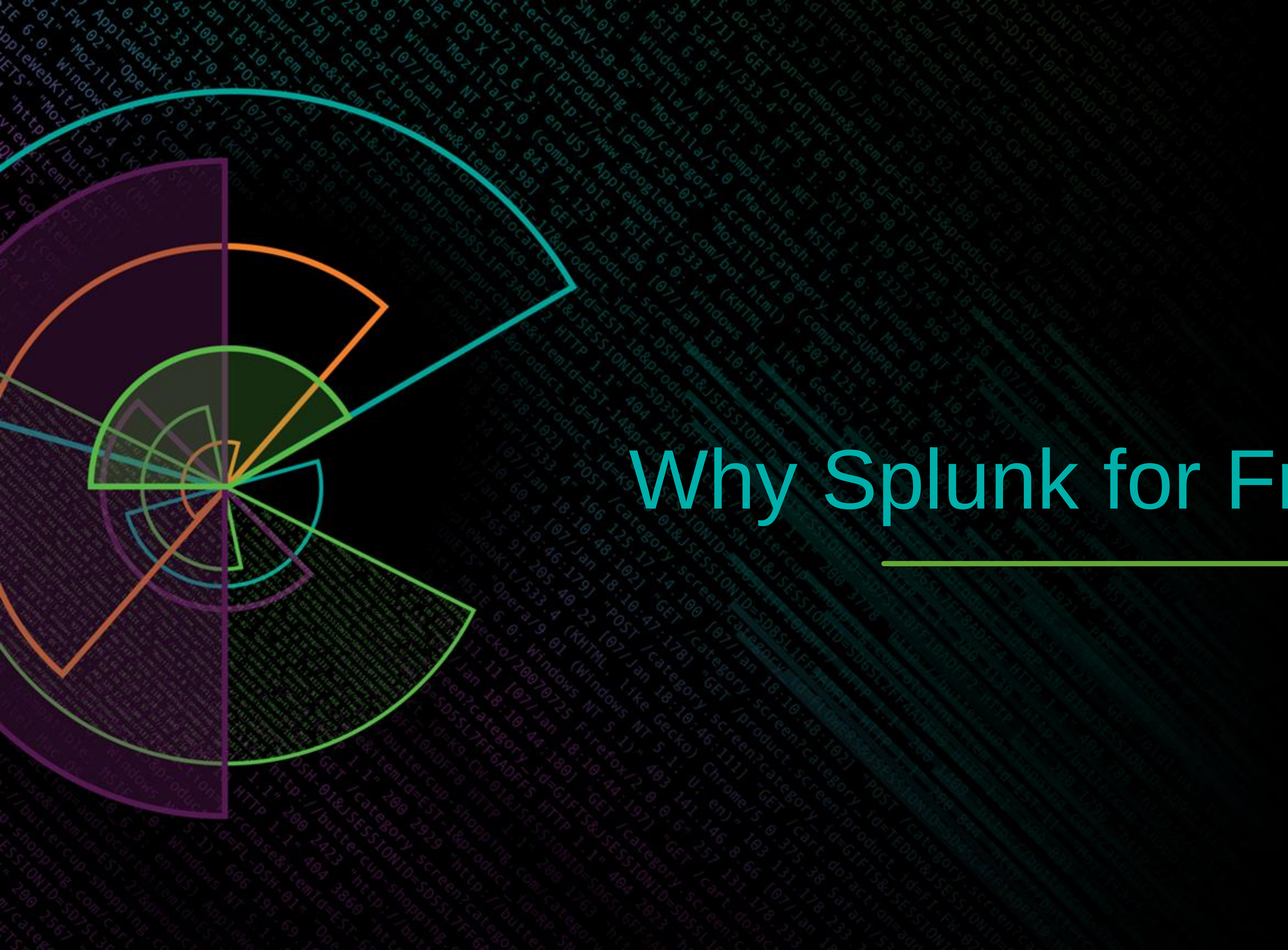
Draft Outline:

- Why Splunk for Fraud (3 min) - Beau
- What is an Account (7 min) - Beau
- Real World SIE Use Cases (25 min) - Grant
- SIE Value / Metrics (5 min) - Grant
- Call to Action (5 min) - Beau

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.



Why Splunk for Fraud?

Existing Fraud Tools Too Limiting

RIGID AND INFLEXIBLE

SCALE AND SPEED ISSUES

NARROW VIEW OF FRAUD

DIFFICULT TO DEPLOY; LIMITED ROI

– Visa CyberSource 2013

Splunk: Leading Solution for Fraud Detection

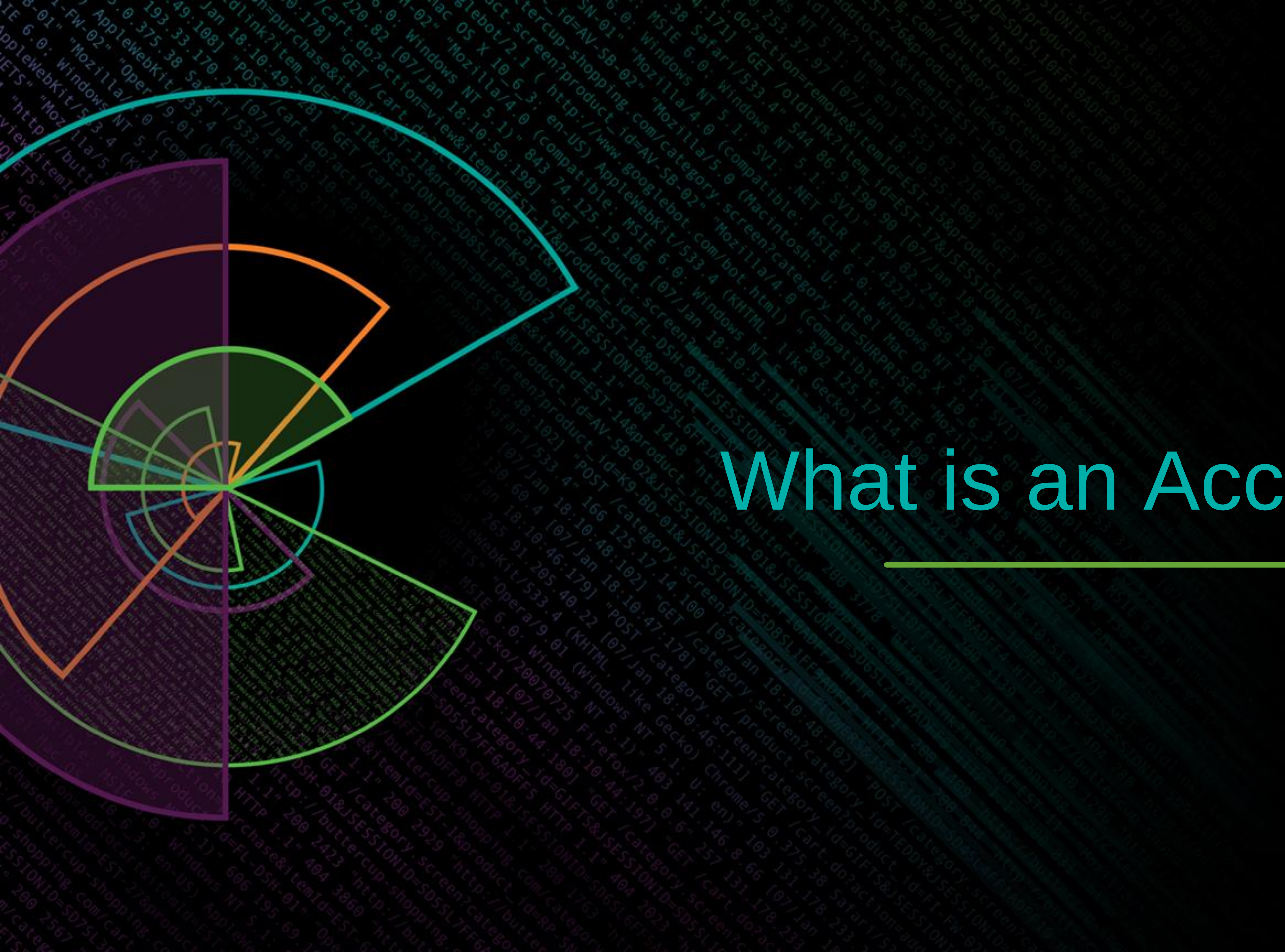
FLEXIBLE

SCALE AND SPEED

splunk>

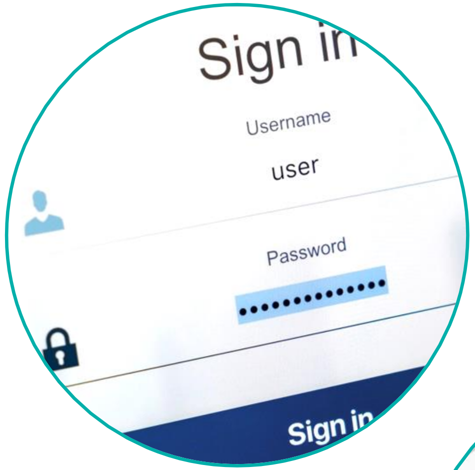
BROAD VIEW

FAST VALUE
COMPELLING ROI



What is an Account?

Accounts Are Customers



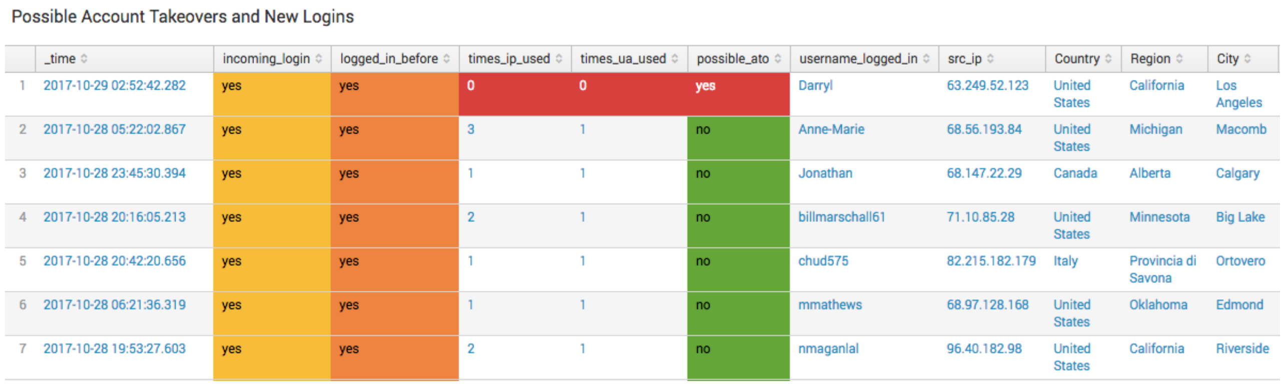
Account Activities

- Transactional (Single Event Type)
  - Credit Card Transactions
  - Inventory Sales
  - Money Movements
  - Loyalty Card
  - Coupons
  - Financial Services

- Behavioral (Multiple Event Types)
  - Online Banking
  - Online Sales
  - Online Insurance
  - Clickstreams
  - Web Logins

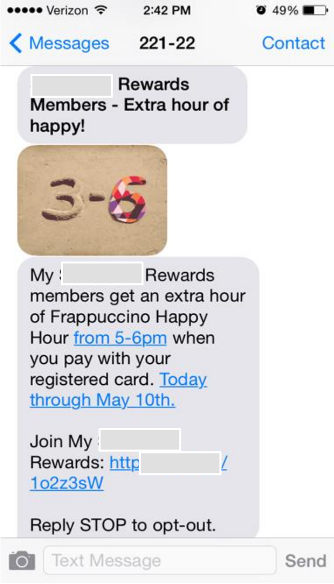
Account Takeover (ATO) Detection Example

Monitor Application Successful Logins from Unusual IPs/Locations to Uncover Successful Phishing



Possible Account Takeovers and New Logins

	_time	incoming_login	logged_in_before	times_ip_used	times_ua_used	possible_ato	username_logged_in	src_ip	Country	Region	City
1	2017-10-29 02:52:42.282	yes	yes	0	0	yes	Darryl	63.249.52.123	United States	California	Los Angeles
2	2017-10-28 05:22:02.867	yes	yes	3	1	no	Anne-Marie	68.56.193.84	United States	Michigan	Macomb
3	2017-10-28 23:45:30.394	yes	yes	1	1	no	Jonathan	68.147.22.29	Canada	Alberta	Calgary
4	2017-10-28 20:16:05.213	yes	yes	2	1	no	billmarschall61	71.10.85.28	United States	Minnesota	Big Lake
5	2017-10-28 20:42:20.656	yes	yes	1	1	no	chud575	82.215.182.179	Italy	Provincia di Savona	Ortovero
6	2017-10-28 06:21:36.319	yes	yes	1	1	no	mmathews	68.97.128.168	United States	Oklahoma	Edmond
7	2017-10-28 19:53:27.603	yes	yes	2	1	no	nmaganlal	96.40.182.98	United States	California	Riverside

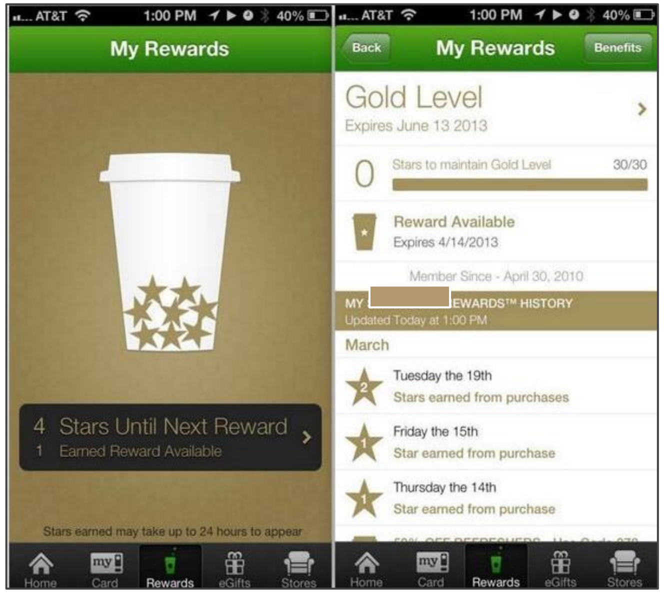


[redacted] Rewards Members - Extra hour of happy!

My [redacted] Rewards members get an extra hour of Frappuccino Happy Hour from 5-6pm when you pay with your registered card. Today through May 10th.

Join My [redacted] Rewards: http[redacted]/ 1o2z3sW

Reply STOP to opt-out.



4 Stars Until Next Reward
1 Earned Reward Available

Stars earned may take up to 24 hours to appear

Gold Level
Expires June 13 2013

0 Stars to maintain Gold Level 30/30

Reward Available
Expires 4/14/2013

Member Since - April 30, 2010

MY [redacted] EWARDS™ HISTORY
Updated Today at 1:00 PM

March

Tuesday the 19th
Stars earned from purchases

Friday the 15th
Star earned from purchase

Thursday the 14th
Star earned from purchase

Real World Use Cases with Real Results

A look at how Sony Interactive Entertainment uses Splunk for Fraud Prevention and Analysis

Introduction

Grant Walthall

Senior Fraud Engineer

Global Fraud Management (GFM)

Sony Interactive Entertainment

Responsibilities of GFM

Financial Fraud

- Real time risk decision making
- Research and monitoring using Splunk and Oracle database

Password List Attack (Credential Stuffing)

Focus of Today

- Detection and password reset of compromised accounts

Account Takeover

- Protection of users accounts
- Recovery of affected accounts

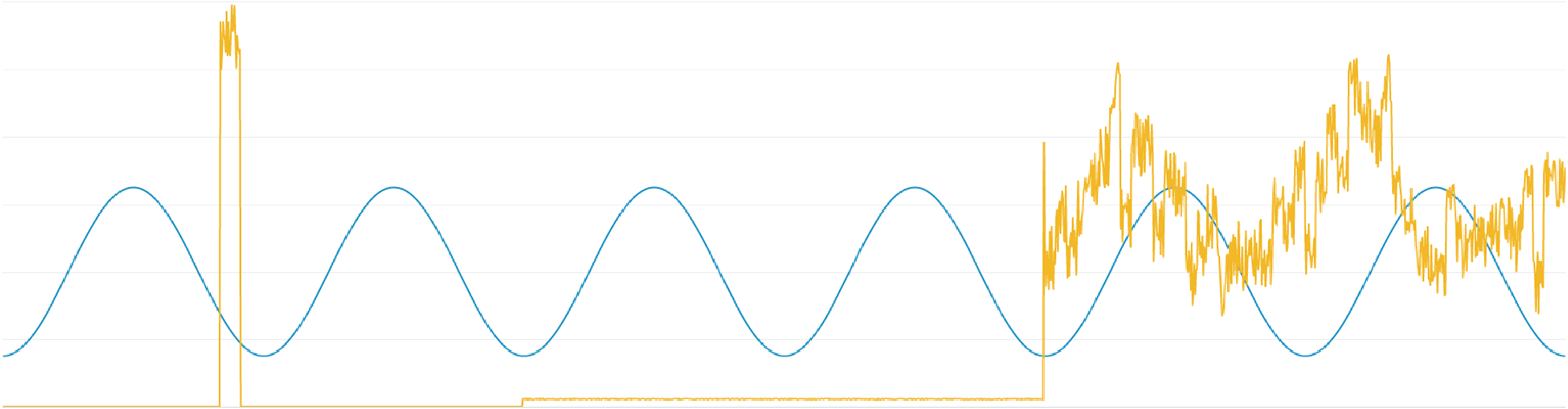
Understanding PLA

Steps of a password list attack

Obtain stolen credentials → **Use botnet to distribute attack** → **Get successful accounts** → **Monetize accounts**

Types of attacks

Massive short term attack | **Low and slow** | **Continuous high volume**



Massive short term attack

- Very simple attack
- Easy to detect

Low and slow

- Attack is not obvious
- Attack is likely continuous

Continuous high volume

- High volume attacks that are unlikely to stop
- usually there are many attacks

Uses of ATO Accounts

- Credit card fraud
- Use of account entitlements
- Use of accounts subscriptions

Depending on the activity hackers may not make any changes to the account.

- Potentially using it at the same time as the owner.

Actions against PLA

Actions Against Password List Attacks

- Security enhancements
  - Prevent unauthorized access
- Rate limiting, IP blocking, and blocking bad requests (WAFs)
  - Limit the scale of the attack
- Password reset
  - Mitigation after the authentication
- Dormant account reset
  - Dormant accounts are at high risk of ATO. We reset the password so that only the account holder can recover the account.

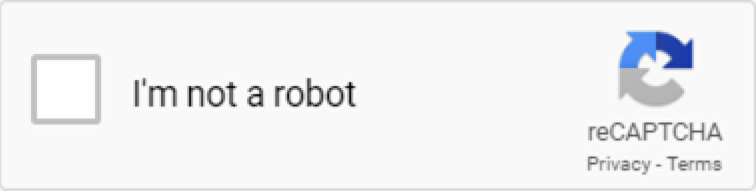
Security Enhancements

Blocking bad authentications is the most desirable action.

- Hackers get an immediate response
- If it is something in their control they will change it

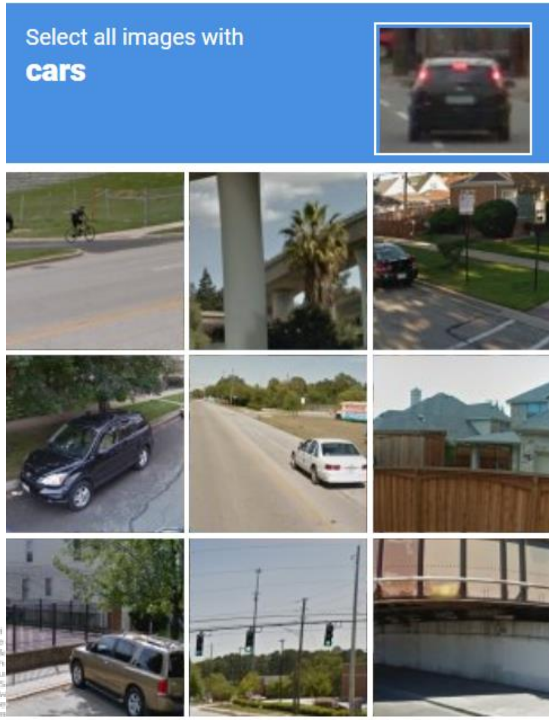
Well thought out enhancements are difficult to work around.

- May cause some friction to users.



Enhancements at SIE:

- Captcha on all authentications
- Two factor authentication
- Machine Learning/biometric detection

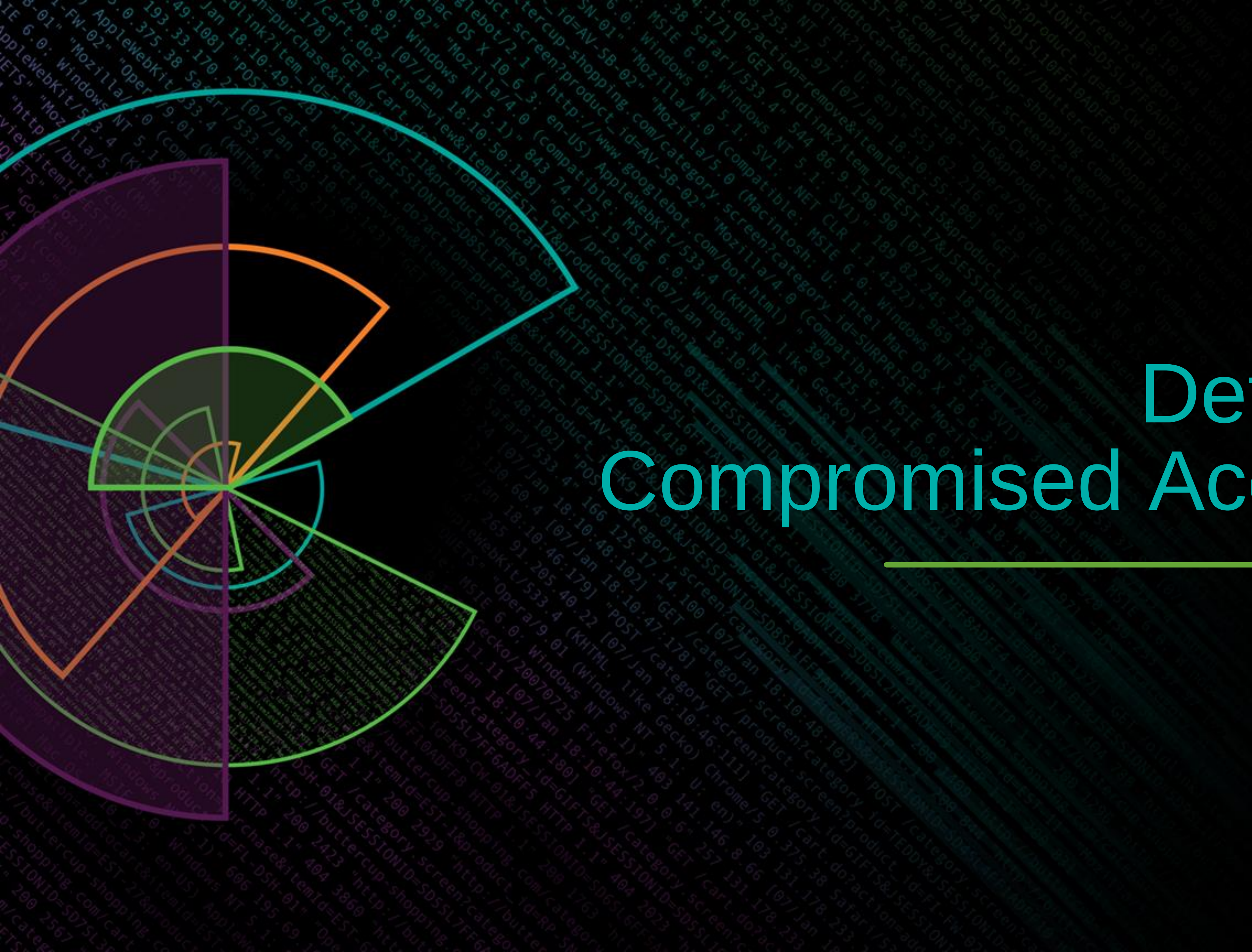


IP Rate Limiting

Rate limiting is important to limit the scale of attacks.

- This may deter some casual hackers.
- Professional hackers will not be deterred.
  - They have a very large number of IP addresses at their disposal.
- Likely has more benefits with DDOS prevention.
- Aggressive rate limiting may make detection harder.

We have seen more than 10 million IP addresses attacking us in a given month



Detecting Compromised Accounts

What can be done?

- You will likely never stop being attacked.
- Blocking attacks can be challenging and expensive.
  - Some will be missed.
- Detection of compromised accounts will always be needed.
  - Splunk has filled this need for us very well.

Useful Data Sources in PLA

Web logs

- Show the behavior of a user or IP address

Authentication logs

- Allows us to know what accounts were actually compromised
- Useful for looking at high failure rates

Other account logs

- Need to know if they have made any other changes
- Email changes are very important to us

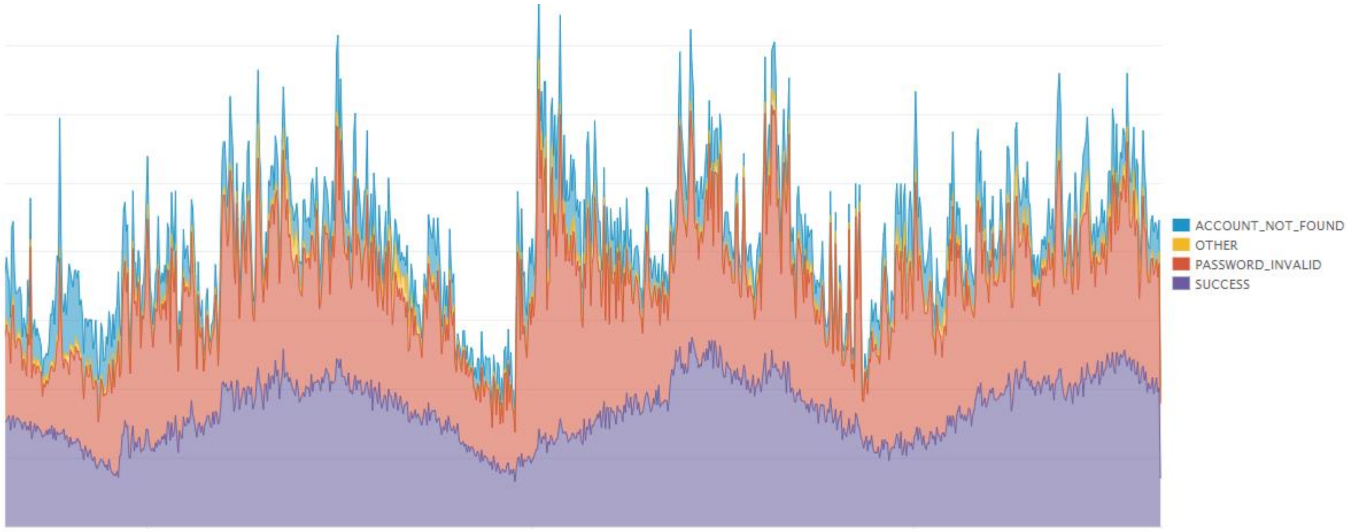
Looking for Potential Attacks

Monitor the following:

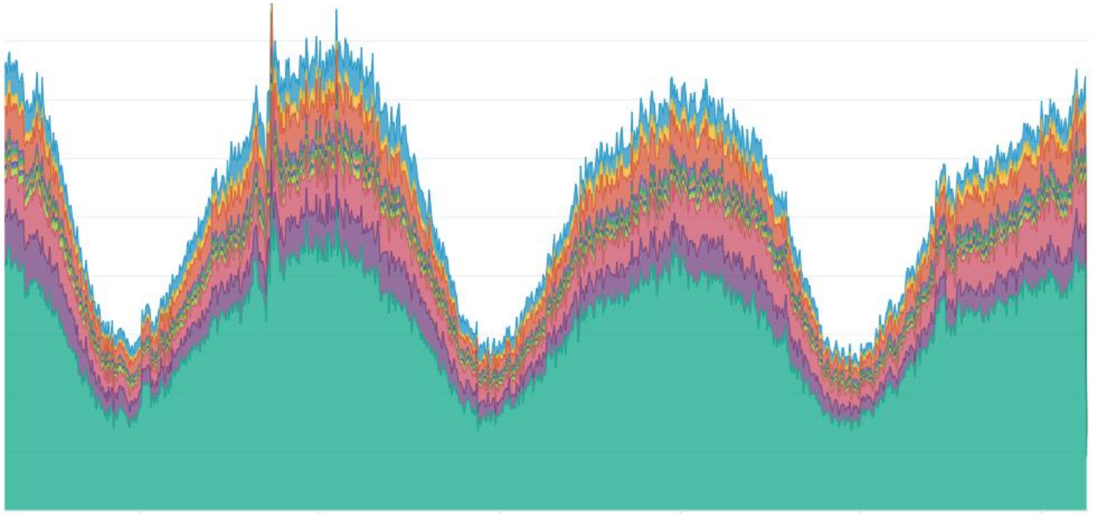
- Authentication endpoints
- Authentication results

<<your data>>
| timechart bins=1000 count by …
user agent, IP country, auth result

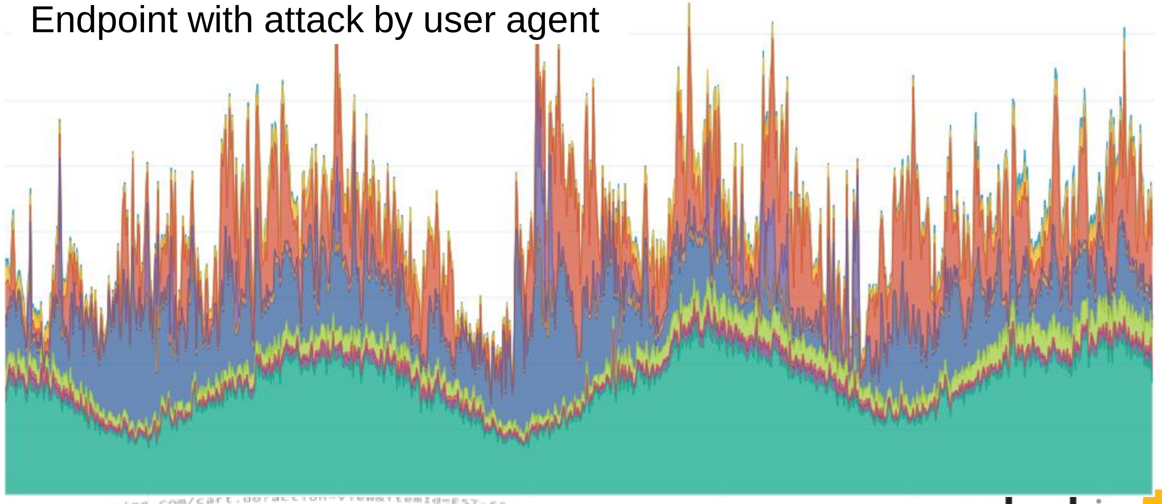
Endpoint with attack by result



Endpoint without an attack by user agent



Endpoint with attack by user agent



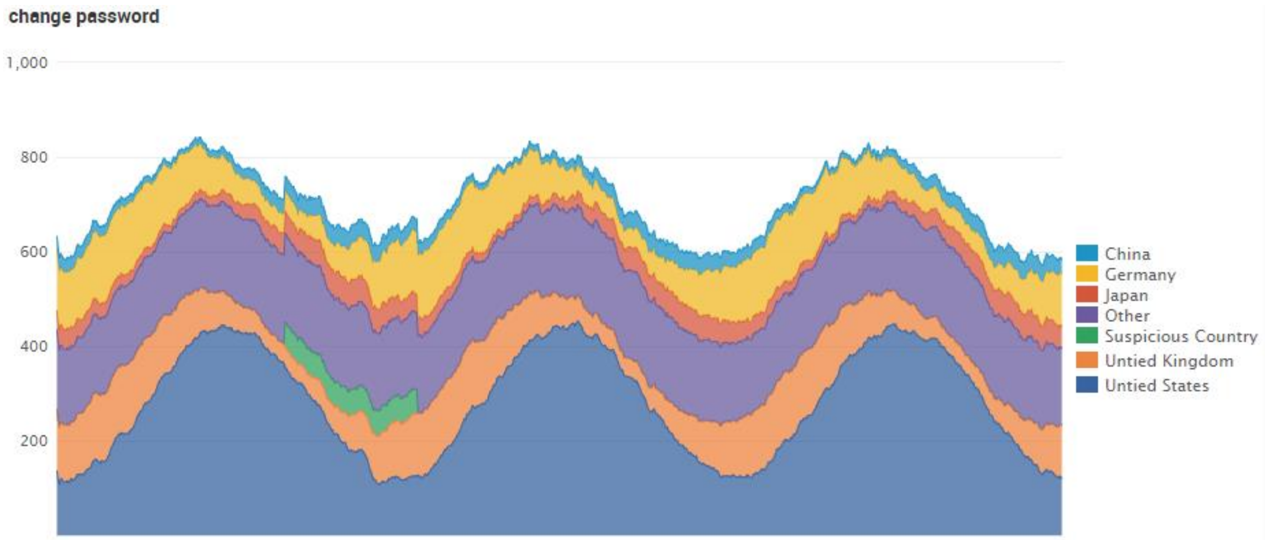
Monitoring Authentications

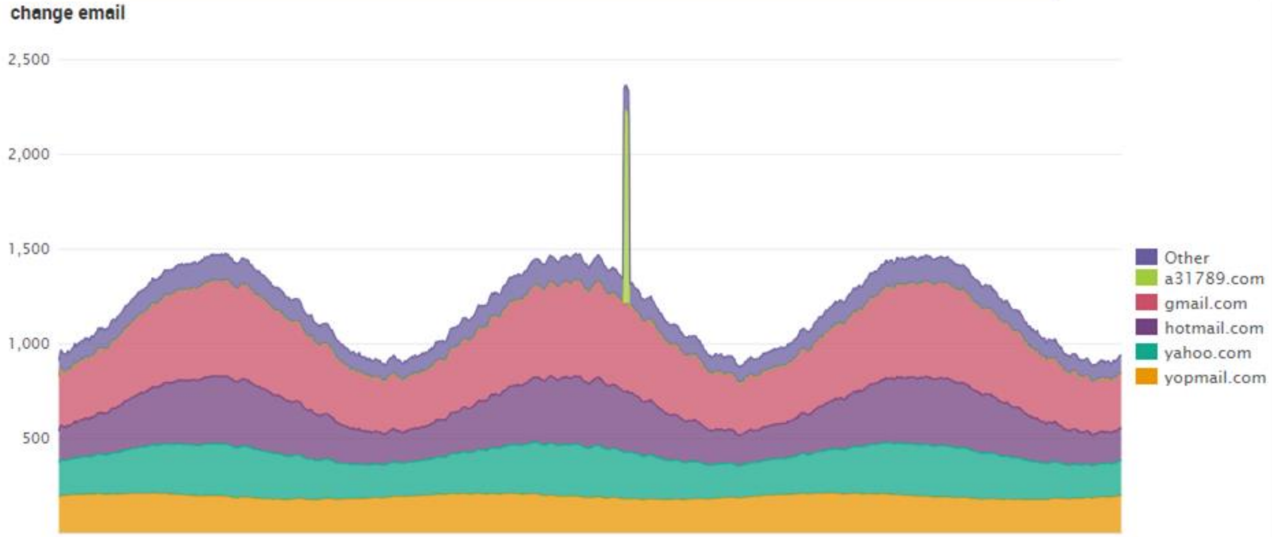
SIE must support a wide range of devices for both current and legacy services.

- Requires greater effort to protect all endpoints from attacks
- Hackers will exploit your weakest endpoints
  - You need to have a good understanding of your network and how they are attacking you
  - Without this we can not make well informed decisions

Monitoring Account Events

- Time charts are helpful in visualizing anomalies
  - Gives us a general idea if there are abnormal activities occuring
- Monitored Events:
  - change password
  - change email
  - add payment instrument
  - sub account creation
  - purchasing events





not actual data

Researching

Splunk is heavily used for researching the scale of new malicious trends and prototyping mitigation.

- We have many different data sources in Splunk
  - This allows us to better understand what is going on and what we can do, which can be very difficult to do in something such as a database.
- Splunk allows for rapid iteration and prototyping

Research steps:

1. Notice anomaly (either through reporting or alerting)
2. Create additional queries looking at suspicious activity

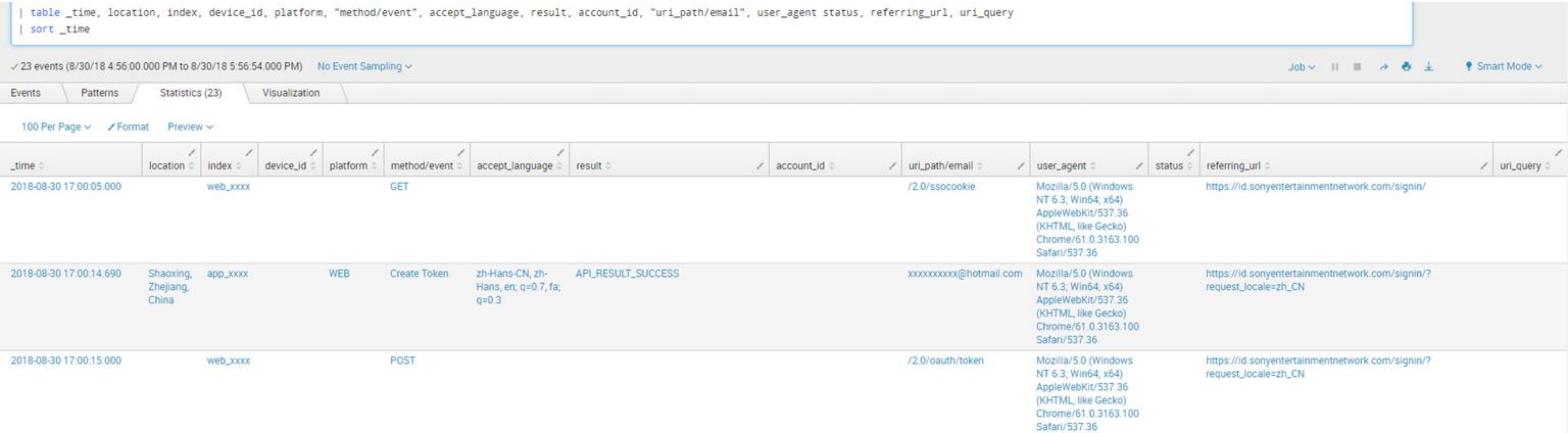
Researching

Try to understand the activity on some data point like IP address, account ID, or session ID.

- Useful to understand how both good users act and hackers act.

Find ways to explore your data that is useful to you.

- This is likely to constantly change.



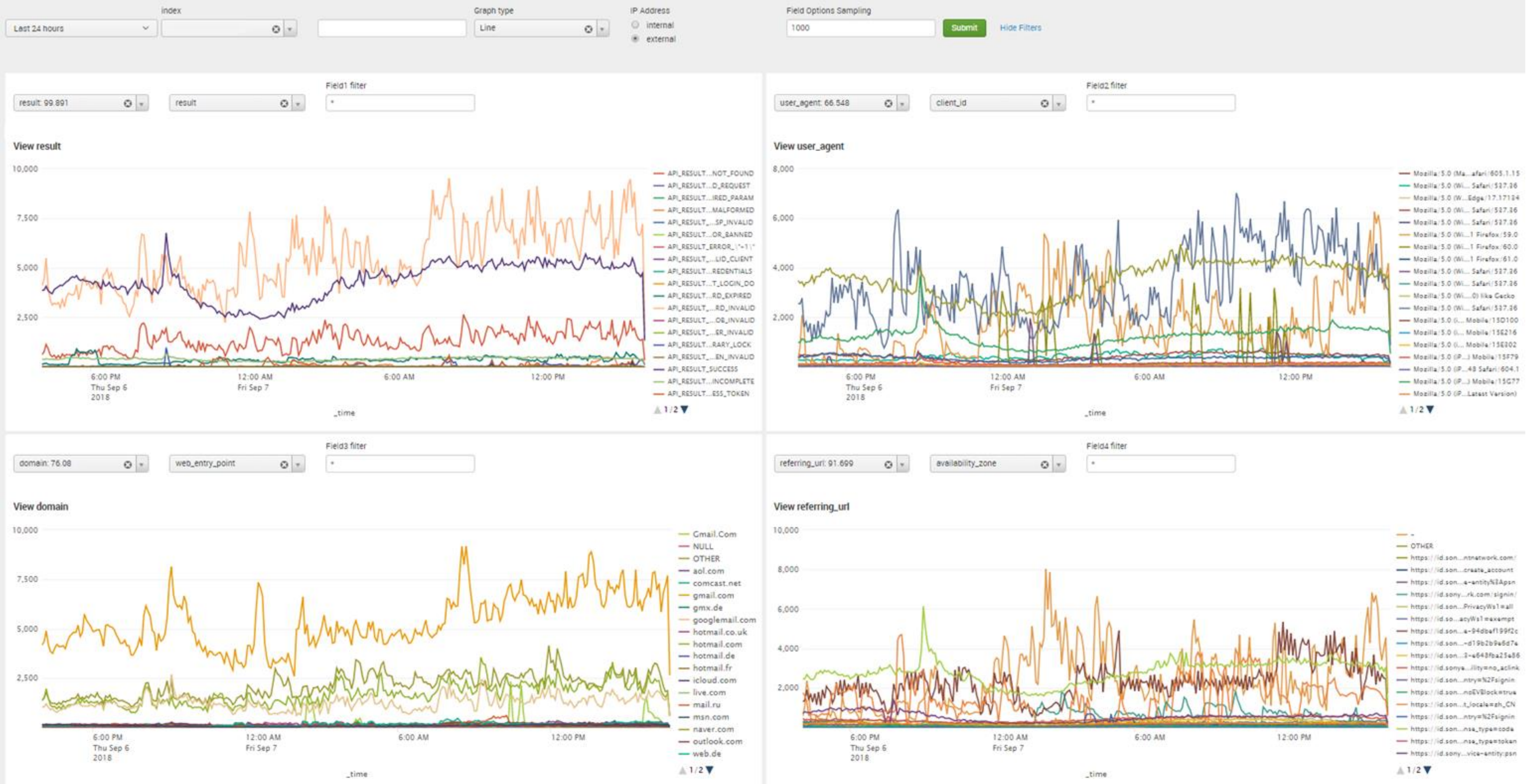
```
| table _time, location, index, device_id, platform, "method/event", accept_language, result, account_id, "uri_path/email", user_agent status, referring_url, uri_query
| sort _time
```

✓ 23 events (8/30/18 4:56:00.000 PM to 8/30/18 5:56:54.000 PM) No Event Sampling

_time	location	index	device_id	platform	method/event	accept_language	result	account_id	uri_path/email	user_agent	status	referring_url	uri_query
2018-08-30 17:00:05.000		web_xxxx			GET				/2.0/ssocookie	Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36		https://id.sonyentertainmentnetwork.com/signin/	
2018-08-30 17:00:14.690	Shaoxing, Zhejiang, China	app_xxxx		WEB	Create Token	zh-Hans-CN, zh-Hans, en; q=0.7, fa; q=0.3	API_RESULT_SUCCESS		xxxxxxxxxx@hotmail.com	Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36		https://id.sonyentertainmentnetwork.com/signin/?request_locale=zh_CN	
2018-08-30 17:00:15.000		web_xxxx			POST				/2.0/oauth/token	Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36		https://id.sonyentertainmentnetwork.com/signin/?request_locale=zh_CN	

Researching

Visuals are often very helpful in understanding your data



Last 24 hours

index:

Graph type: Line

IP Address: ○ internal ● external

Field Options Sampling: 1000

Submit

Hide Filters

result: 99.891 | result | Field1 filter: *

user_agent: 66.548 | client_id | Field2 filter: *

domain: 76.08 | web_entry_point | Field3 filter: *

referring_url: 91.699 | availability_zone | Field4 filter: *

View result
10,000
7,500
5,000
2,500
6:00 PM
Thu Sep 6
2018
12:00 AM
Fri Sep 7
6:00 AM
12:00 PM
_time
API_RESULT...NOT_FOUND
API_RESULT...D_REQUEST
API_RESULT...IRED_PARAM
API_RESULT...MALFORMED
API_RESULT_...SP_INVALID
API_RESULT...OR_BANNED
API_RESULT_ERROR_\"-1\"
API_RESULT_...LID_CLIENT
API_RESULT...REDENTIALS
API_RESULT...T_LOGIN_DO
API_RESULT...RD_EXPIRED
API_RESULT_...RD_INVALID
API_RESULT_...OB_INVALID
API_RESULT_...ER_INVALID
API_RESULT...RARY_LOCK
API_RESULT_...EN_INVALID
API_RESULT_SUCCESS
API_RESULT...INCOMPLETE
API_RESULT...ESS_TOKEN
1/2
View user_agent
8,000
6,000
4,000
2,000
6:00 PM
Thu Sep 6
2018
12:00 AM
Fri Sep 7
6:00 AM
12:00 PM
_time
Mozilla/5.0 (Ma...afari/605.1.15
Mozilla/5.0 (Wi... Safari/537.36
Mozilla/5.0 (W...Edge/17.17134
Mozilla/5.0 (Wi... Safari/537.36
Mozilla/5.0 (Wi... Safari/537.36
Mozilla/5.0 (Wi...1 Firefox/59.0
Mozilla/5.0 (Wi...1 Firefox/60.0
Mozilla/5.0 (Wi...1 Firefox/61.0
Mozilla/5.0 (Wi... Safari/537.36
Mozilla/5.0 (Wi... Safari/537.36
Mozilla/5.0 (Wi....0) like Gecko
Mozilla/5.0 (Wi... Safari/537.36
Mozilla/5.0 (i... Mobile/15D100
Mozilla/5.0 (i... Mobile/15E216
Mozilla/5.0 (i... Mobile/15E302
Mozilla/5.0 (iP...) Mobile/15F79
Mozilla/5.0 (iP...48 Safari/604.1
Mozilla/5.0 (iP...) Mobile/15G77
Mozilla/5.0 (iP...Latest Version)
1/2
View domain
10,000
7,500
5,000
2,500
6:00 PM
Thu Sep 6
2018
12:00 AM
Fri Sep 7
6:00 AM
12:00 PM
_time
Gmail.Com
NULL
OTHER
aol.com
comcast.net
gmail.com
gmx.de
googlemail.com
hotmail.co.uk
hotmail.com
hotmail.de
hotmail.fr
icloud.com
live.com
mail.ru
msn.com
naver.com
outlook.com
web.de
1/2
View referring_url
10,000
8,000
6,000
4,000
2,000
6:00 PM
Thu Sep 6
2018
12:00 AM
Fri Sep 7
6:00 AM
12:00 PM
_time
-
OTHER
https://id.son...ntnetwork.com/
https://id.son...create_account
https://id.son...e-entity%3Apsn
https://id.sony...rk.com/signin/
https://id.son...PrivacyWs1=all
https://id.so...acyWs1=exempt
https://id.son...e-94dbaf199f2c
https://id.son...-d19b2b9e6d7e
https://id.son...3-e643fba25e86
https://id.sonye...ility=no_aclink
https://id.son...ntry=%2Fsignin
https://id.son...noEVBlock=true
https://id.son...t_locale=zh_CN
https://id.son...ntry=%2Fsignin
https://id.son...nse_type=code
https://id.son...nse_type=token
https://id.sony...vice-entity:psn
1/2

splunk> .conf18

Some SIE Detections

SIE detection rules (typically on IP):

- High failure to success ratio
- Skipping endpoints
  - For example skipping login page and hitting authentication endpoint directly
- High counts of endpoints that are rarely used
  - Hackers evaluate what values an account has, such as what games it owns
  - Other account information may also be evaluated
- Accounts on many IP addresses
  - As well as other accounts on those IP addresses
- Many authentications occurring very quickly

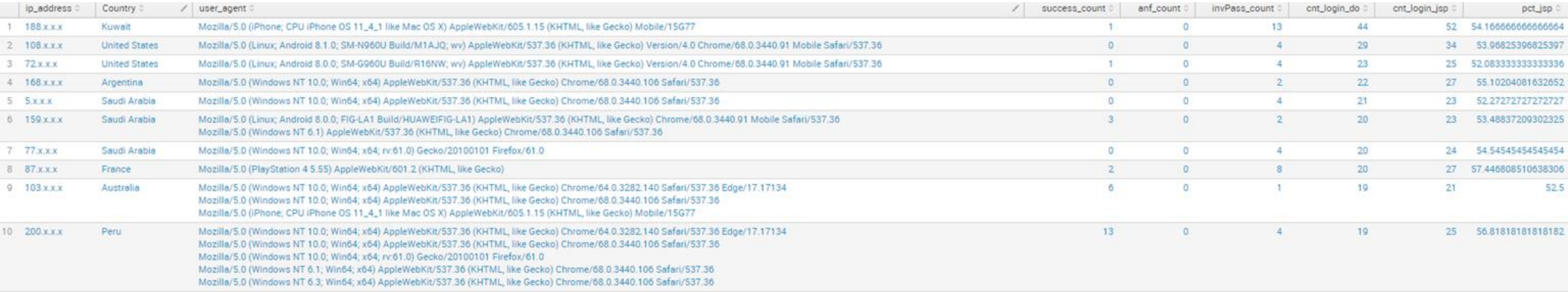
Detection Process

Iteration is very important

- Which Splunk is great at

Output any data that may be relevant for either detection or validation

- For example user agent is not great for detection, but can be very useful for validation when developing rules



	ip_address	Country	user_agent	success_count	anf_count	invPass_count	cnt_login_do	cnt_login_jsp	pct_jsp
1	188.x.x.x	Kuwait	Mozilla/5.0 (iPhone; CPU iPhone OS 11_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15G77	1	0	13	44	52	54.166666666666664
2	108.x.x.x	United States	Mozilla/5.0 (Linux; Android 8.1.0; SM-N960U Build/M1AJQ; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/68.0.3440.91 Mobile Safari/537.36	0	0	4	29	34	53.96825396825397
3	72.x.x.x	United States	Mozilla/5.0 (Linux; Android 8.0.0; SM-G960U Build/R16NW; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/68.0.3440.91 Mobile Safari/537.36	1	0	4	23	25	52.083333333333336
4	168.x.x.x	Argentina	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36	0	0	2	22	27	55.10204081632652
5	5.x.x.x	Saudi Arabia	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36	0	0	4	21	23	52.27272727272727
6	159.x.x.x	Saudi Arabia	Mozilla/5.0 (Linux; Android 8.0.0; FIG-LA1 Build/HUAWEIFIG-LA1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.91 Mobile Safari/537.36 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36	3	0	2	20	23	53.48837209302325
7	77.x.x.x	Saudi Arabia	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0	0	0	4	20	24	54.54545454545454
8	87.x.x.x	France	Mozilla/5.0 (PlayStation 4 5.55) AppleWebKit/601.2 (KHTML, like Gecko)	2	0	8	20	27	57.446808510638306
9	103.x.x.x	Australia	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36 Mozilla/5.0 (iPhone; CPU iPhone OS 11_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mobile/15G77	6	0	1	19	21	52.5
10	200.x.x.x	Peru	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36 Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0 Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36 Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36	13	0	4	19	25	56.81818181818182

Detection Process

Detection Research

```
(<<web data>>) OR (<<authentication data>>)
| iplocation ip_address
| stats
  values(Country) as Country
  values(user_agent) as user_agent
  count(eval(result like "%SUCCESS")) as success_count
  count(eval(result like "%ACCOUNT_NOT_FOUND ")) as
anf_count
  count(eval(result like "%INVALID_PASSWORD")) as
invPass_count
  count(eval(match(uri_path,"<<auth endpoint>>"))) as cnt_auth
  count(eval(match(uri_path,"<<login page>>))) as cnt_login_page
by ip_address
| where cnt_auth > 0 AND
(success_count+anf_count+invPass_count) > 0
| eval
pct_login_page=(cnt_login_page/(cnt_auth+cnt_login_page))*100
| sort - cnt_auth
```

More data is returned in order to determine what is even relevant.

Finalized detection

```
(<<web data>>) OR (<<authentication data>>)
| iplocation ip_address
| stats
  count(result) as authentications
  count(eval(match(uri_path,"^<<auth endpoint>>"))) as cnt_auth
  count(eval(match(uri_path,"<<login page>>"))) as cnt_login_page
by ip_address
| where cnt_auth > 0 AND authentications> 0
| eval
pct_login_page=(cnt_login_page/(cnt_auth+cnt_login_page))*100
| where pct_jsp<20 AND cnt_auth>=5
```

Only data relevant to detection is returned.

Data sent to summary index.

Detection Process

Using detected bad IPs

```
(index=<<summary index>> source=<<search name of IP
detection>>) OR (<<auth data>> result=*SUCCESS)
| eval account=_time.":".account_id.":".sign_in_id
| stats
  values(account) as account
  count(eval(index="<<summary index>>")) as cnt_bad
by ip_address
| where cnt_bad>0
| mvexpand account
| rex field=account
"^(?<_time>\d+(\.\d+)?):(?<account_id>\d+):(?<sign_in_id>.*)$"
| stats
  first(sign_in_id) as sign_in_id
  min(_time) as _time
  values(ip_address) as ip_address
  count as cnt_auth
  dc(ip_address) as dc_ip
by account_id
| eval ip_address=mvindex(ip_address,0,9)
```

Identifying accounts in same search

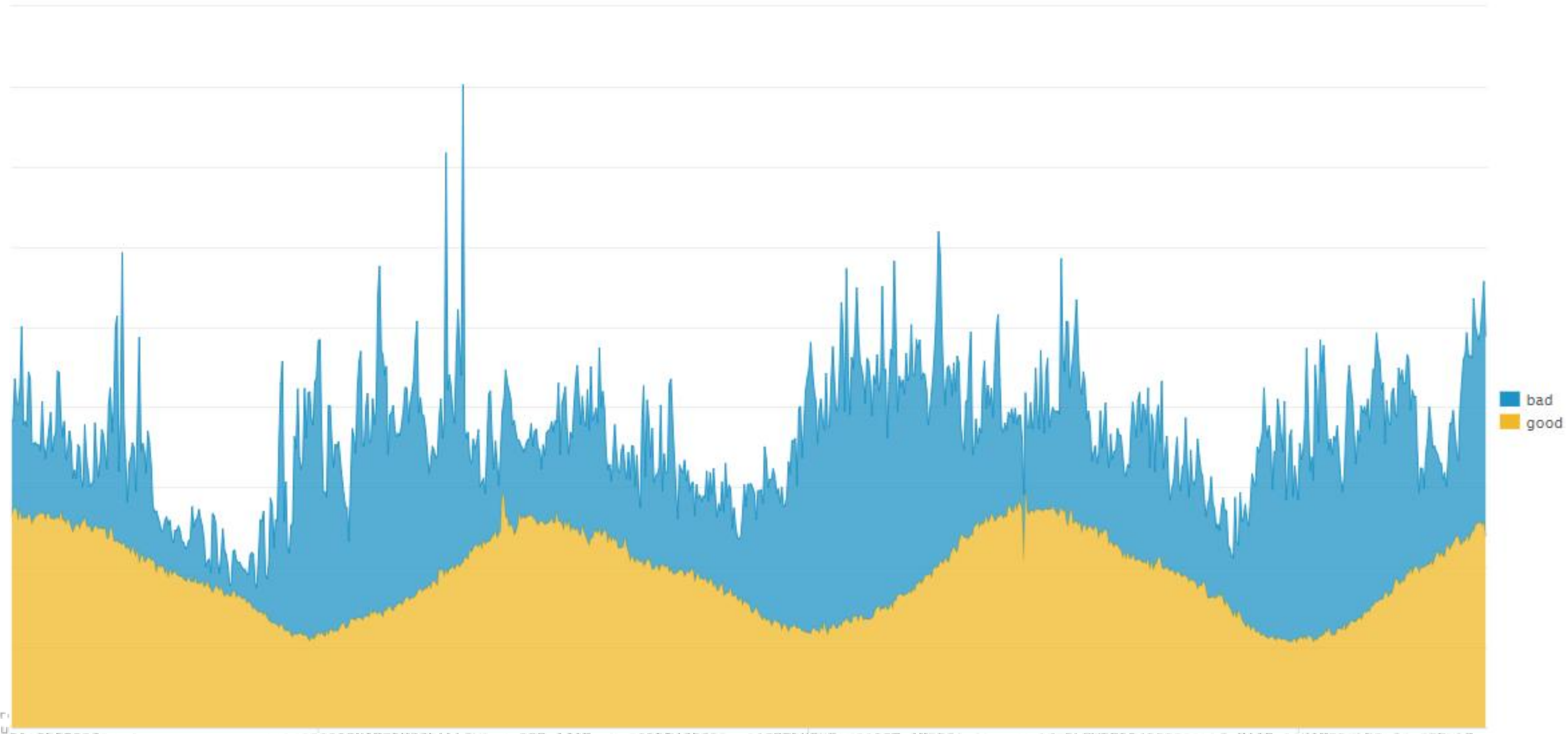
```
(<<web data>>)
OR (<<auth data>> result=*SUCCESS)
| eval user=account_id."|".sign_in_id
| stats
  count(eval(result like "%SUCCESS")) as success_count
  values(user) as user
  count(eval(match(uri_path,"^<<auth endpoint>>"))) as cnt_auth
  count(eval(match(uri_path,"<<login page>>"))) as
cnt_login_page
by ip_address
| eval
pct_login_page=(cnt_login_page/(cnt_auth+cnt_login_page))*100
| where pct_jsp<20 AND cnt_auth>=5
| fields ip_address user
| mvexpand user
| rex field=user "^(?<account_id>\d+)\|(?<sign_in_id>.*)$"
| table account_id sign_in_id ip_address
```

Validation of Detection

Identify data useful for determining false positives and false negatives

- Not recommended to be data used in the rule
- User agent and IP location have been helpful

Graph the data using a timechart to see if the results look as you might expect

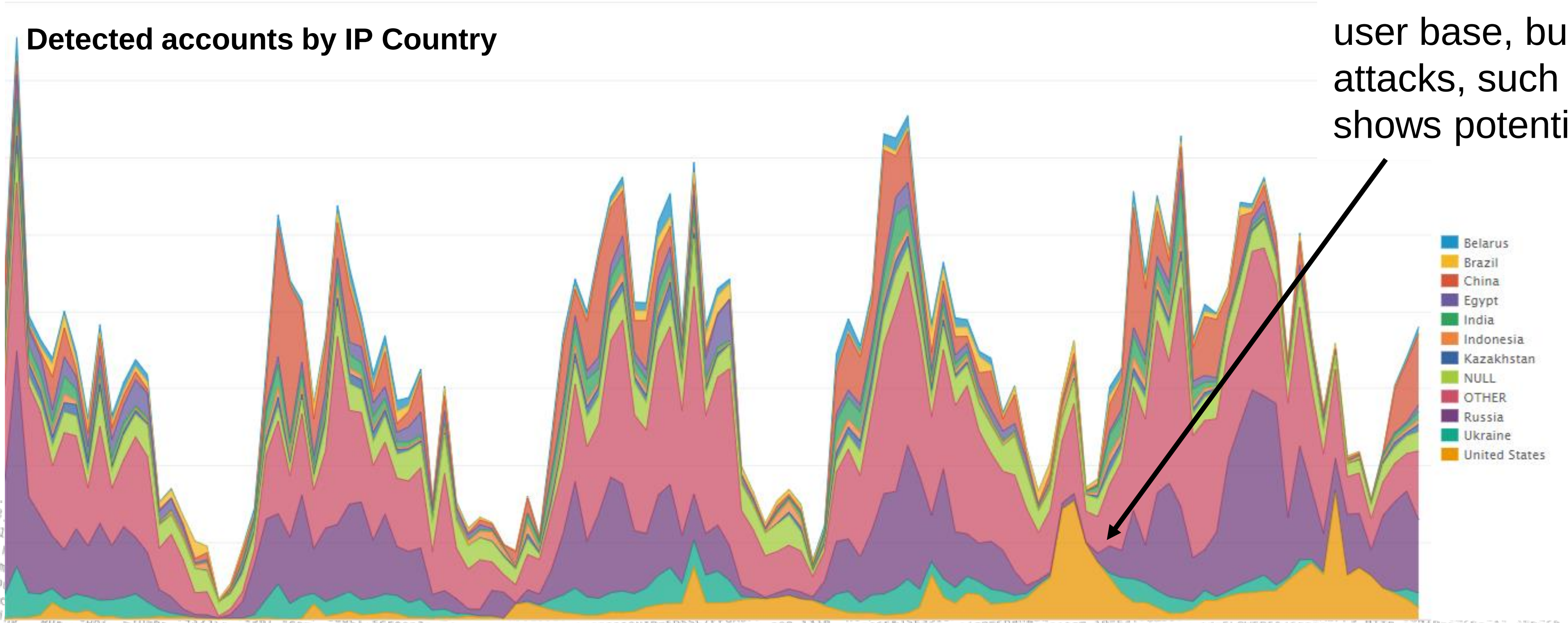


Monitor Detection

Useful in understanding if significant amounts of missed accounts

Helpful in determining false positive events

- Looking at the IP country is often helpful for this



An increase in countries with a large user base, but uncommon for attacks, such as the United States, shows potential false positives.

PLA mitigation

Detecting Accounts

Direct detection

- Identifying compromised account solely from logs for those accounts

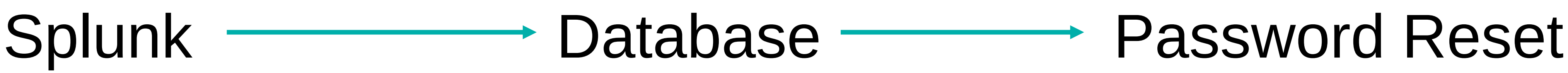
Correlating detection

- Identifying IP addresses, devices, or other criteria
- Every account using that IP, device, etc. is identified as compromised
- If the time period is too long you will have a greater degree of false positives
  - Due to botnets being comprised of compromised devices, our users will sometimes have a compromised device on their IP address

Challenges in Splunk

A challenge we faced was the ability to perform some lookups in Splunk.

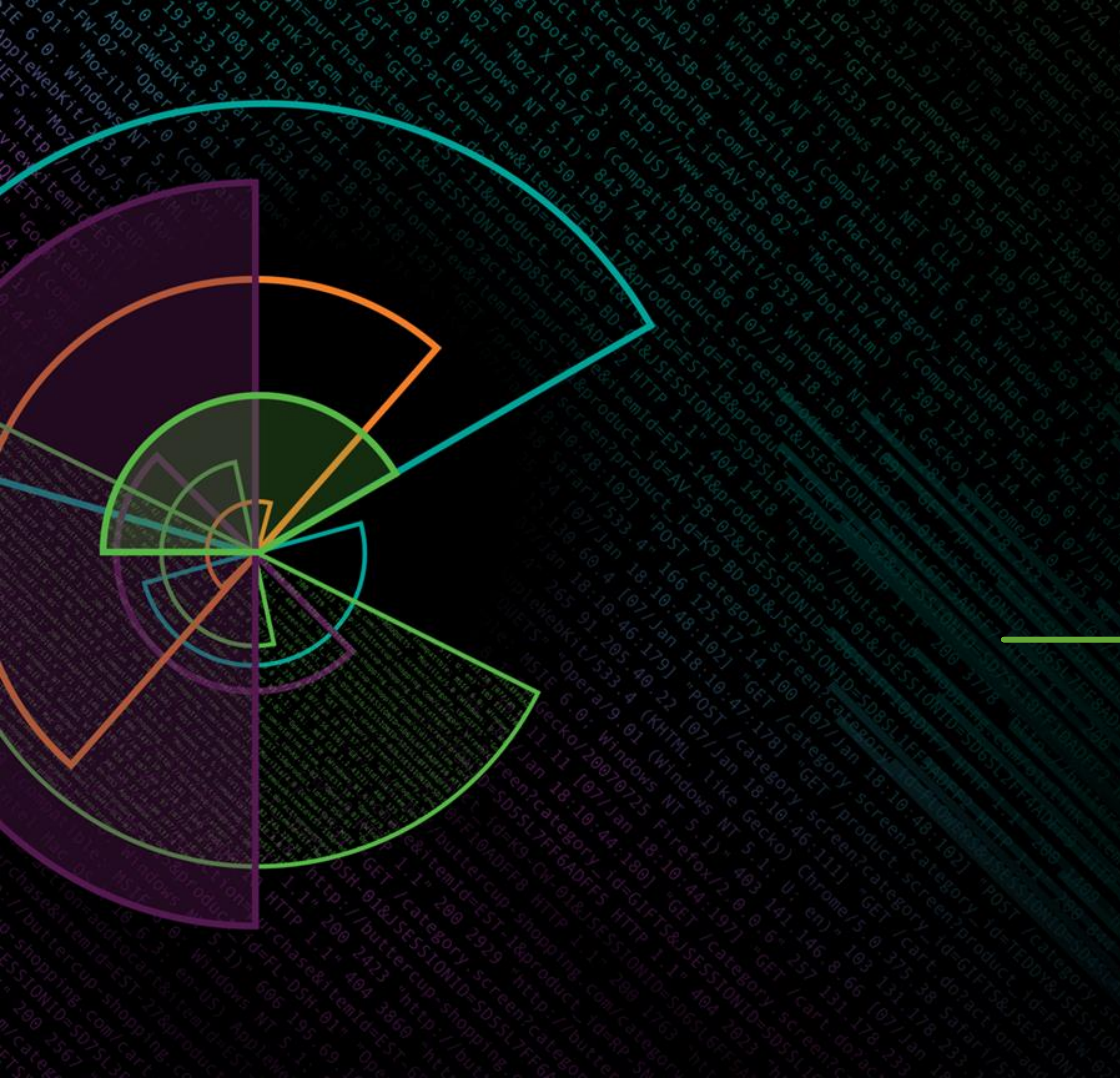
- For example our account table is massive and is constantly updated.
- We solved this problem by sending data from Splunk to a database to do these lookups.



Splunk → Database → Password Reset

Where to Start?

- Monitoring data
- Identifying bad/suspicious activities
- Identify what can and needs to be done to affected accounts



Call to Action

What’s Next?

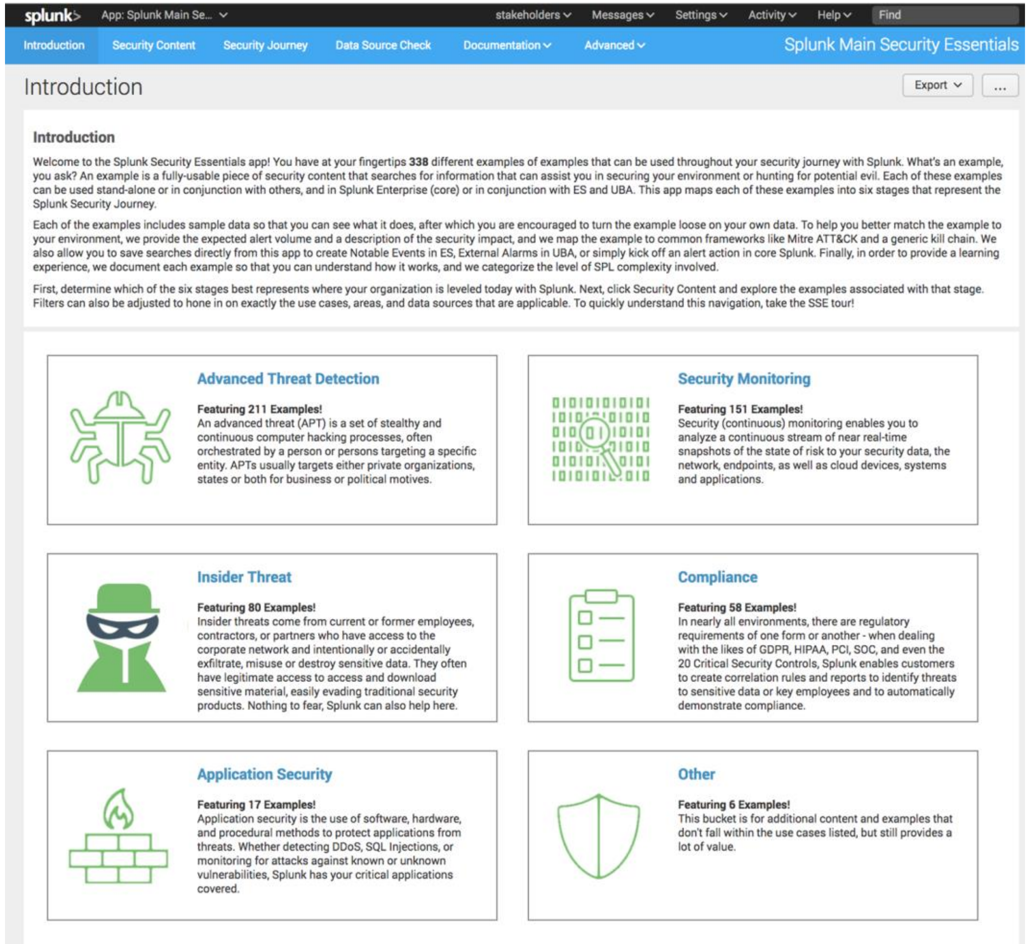
Splunk Security Essentials

https://splunkbase.splunk.com/app/3435/

Learn to improve your security using Splunk's analytics-driven security:

✓Common use cases and examples to get started
✓Data onboarding guide for top data sources
✓Understand how to improve your security
✓Scales from small to massive companies
✓Save searches, send results to ES/UBA

You can learn to solve use cases today for free, then use with Splunk solutions



Introduction

Introduction

Welcome to the Splunk Security Essentials app! You have at your fingertips **338** different examples of examples that can be used throughout your security journey with Splunk. What's an example, you ask? An example is a fully-usable piece of security content that searches for information that can assist you in securing your environment or hunting for potential evil. Each of these examples can be used stand-alone or in conjunction with others, and in Splunk Enterprise (core) or in conjunction with ES and UBA. This app maps each of these examples into six stages that represent the Splunk Security Journey.

Each of the examples includes sample data so that you can see what it does, after which you are encouraged to turn the example loose on your own data. To help you better match the example to your environment, we provide the expected alert volume and a description of the security impact, and we map the example to common frameworks like Mitre ATT&CK and a generic kill chain. We also allow you to save searches directly from this app to create Notable Events in ES, External Alarms in UBA, or simply kick off an alert action in core Splunk. Finally, in order to provide a learning experience, we document each example so that you can understand how it works, and we categorize the level of SPL complexity involved.

First, determine which of the six stages best represents where your organization is leveled today with Splunk. Next, click Security Content and explore the examples associated with that stage. Filters can also be adjusted to hone in on exactly the use cases, areas, and data sources that are applicable. To quickly understand this navigation, take the SSE tour!

Advanced Threat Detection

Featuring 211 Examples!
An advanced threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity. APTs usually targets either private organizations, states or both for business or political motives.

Security Monitoring

Featuring 151 Examples!
Security (continuous) monitoring enables you to analyze a continuous stream of near real-time snapshots of the state of risk to your security data, the network, endpoints, as well as cloud devices, systems and applications.

Insider Threat

Featuring 80 Examples!
Insider threats come from current or former employees, contractors, or partners who have access to the corporate network and intentionally or accidentally exfiltrate, misuse or destroy sensitive data. They often have legitimate access to access and download sensitive material, easily evading traditional security products. Nothing to fear, Splunk can also help here.

Compliance

Featuring 58 Examples!
In nearly all environments, there are regulatory requirements of one form or another - when dealing with the likes of GDPR, HIPAA, PCI, SOC, and even the 20 Critical Security Controls, Splunk enables customers to create correlation rules and reports to identify threats to sensitive data or key employees and to automatically demonstrate compliance.

Application Security

Featuring 17 Examples!
Application security is the use of software, hardware, and procedural methods to protect applications from threats. Whether detecting DDoS, SQL Injections, or monitoring for attacks against known or unknown vulnerabilities, Splunk has your critical applications covered.

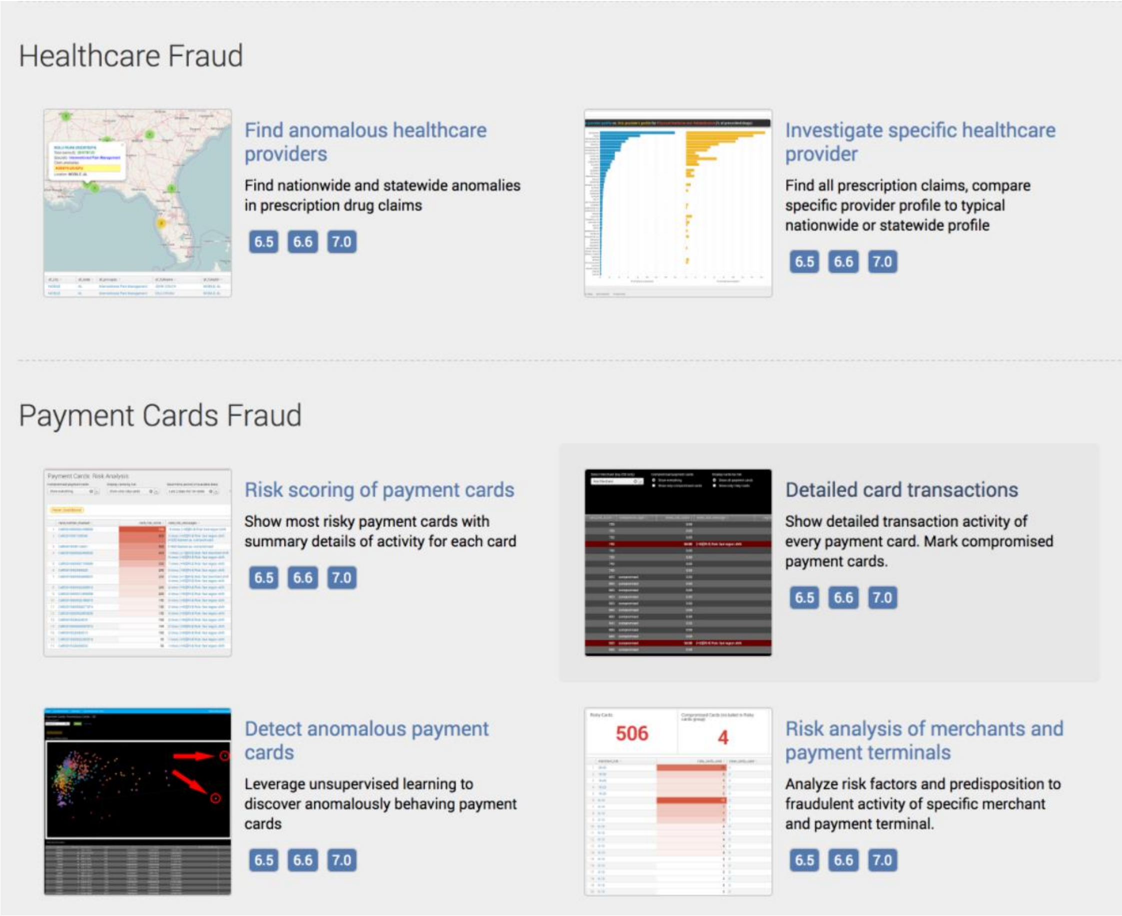
Other

Featuring 6 Examples!
This bucket is for additional content and examples that don't fall within the use cases listed, but still provides a lot of value.

Splunk Essentials for Fraud Detection

https://splunkbase.splunk.com/app/3693/

Learn how Splunk Enterprise may be used to detect various forms of fraud using the example scenarios.



Healthcare Fraud

Find anomalous healthcare providers

Find nationwide and statewide anomalies in prescription drug claims

6.5 6.6 7.0

Investigate specific healthcare provider

Find all prescription claims, compare specific provider profile to typical nationwide or statewide profile

6.5 6.6 7.0

Payment Cards Fraud

Risk scoring of payment cards

Show most risky payment cards with summary details of activity for each card

6.5 6.6 7.0

Detailed card transactions

Show detailed transaction activity of every payment card. Mark compromised payment cards.

6.5 6.6 7.0

Detect anomalous payment cards

Leverage unsupervised learning to discover anomalously behaving payment cards

6.5 6.6 7.0

Risk analysis of merchants and payment terminals

Analyze risk factors and predisposition to fraudulent activity of specific merchant and payment terminal.

6.5 6.6 7.0

Free Workshops

Deep-dive and grow your fraud detection skills

- Beginning Fraud Detection
- Advanced Fraud Detection
- Threat Hunting Workshop
- Boss of the SOC v2

Thank You

Don't forget to rate this session
in the .conf18 mobile app

.conf18

splunk>