Splunking around the Phishmas Tree

SEC1494

Technical Session

.conf25

splunk>

Forward-looking statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk> .conf25

Why am I here?

Splunking around the Phishmas Tree

Steve Behm

Solutions Engineer | Security Researcher
DomainTools
LinkedIn

.conf25
splunk>

How can this story help you?

1

Stay ahead of emerging threats

2

Reduce risk exposure

3

Improve team efficiency

Learning Objectives

Pivot on data points to expand visibility

Create a search to find the threat actor's domains

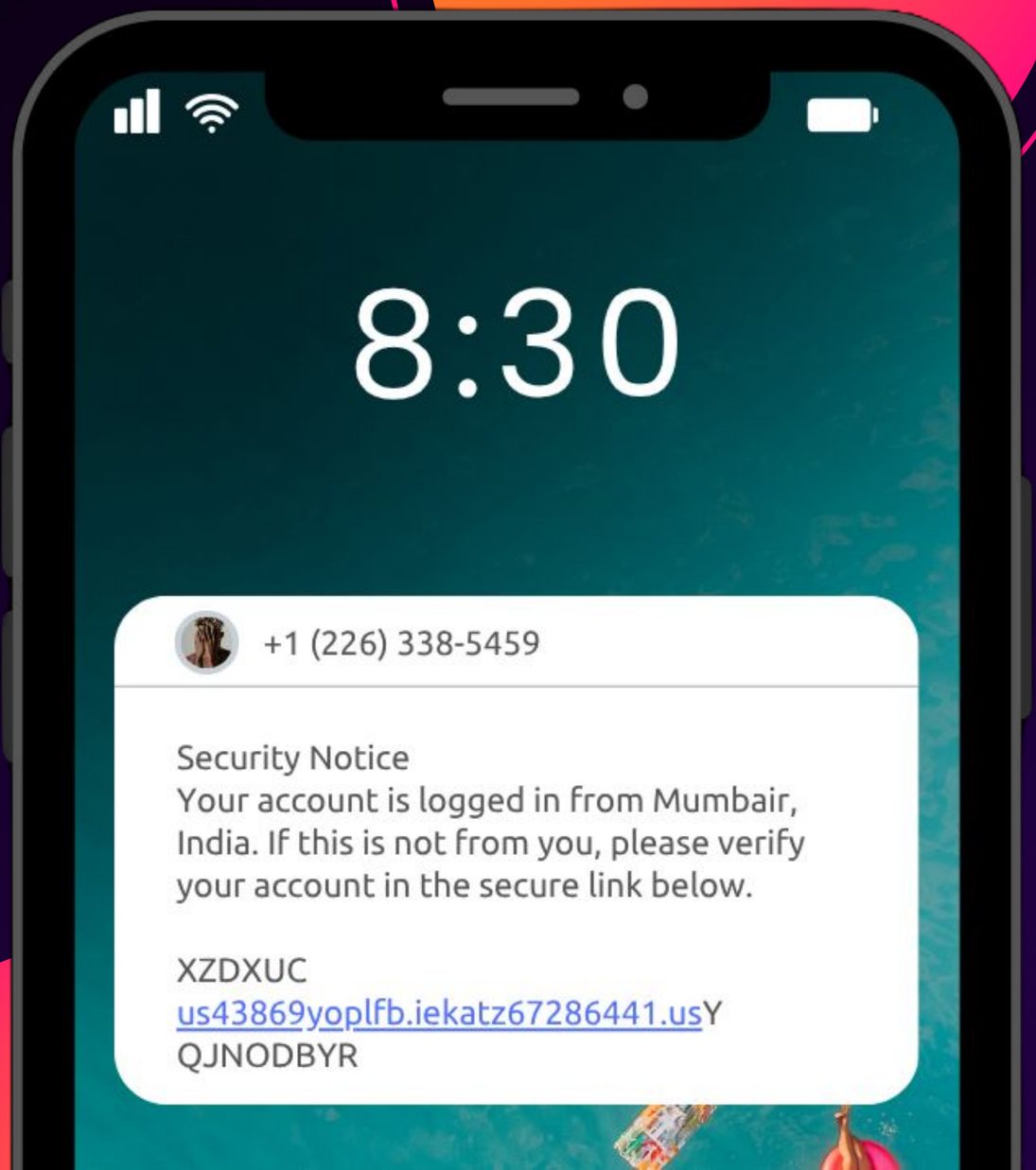
Automate the search to run regularly

Explore last mile possibilities

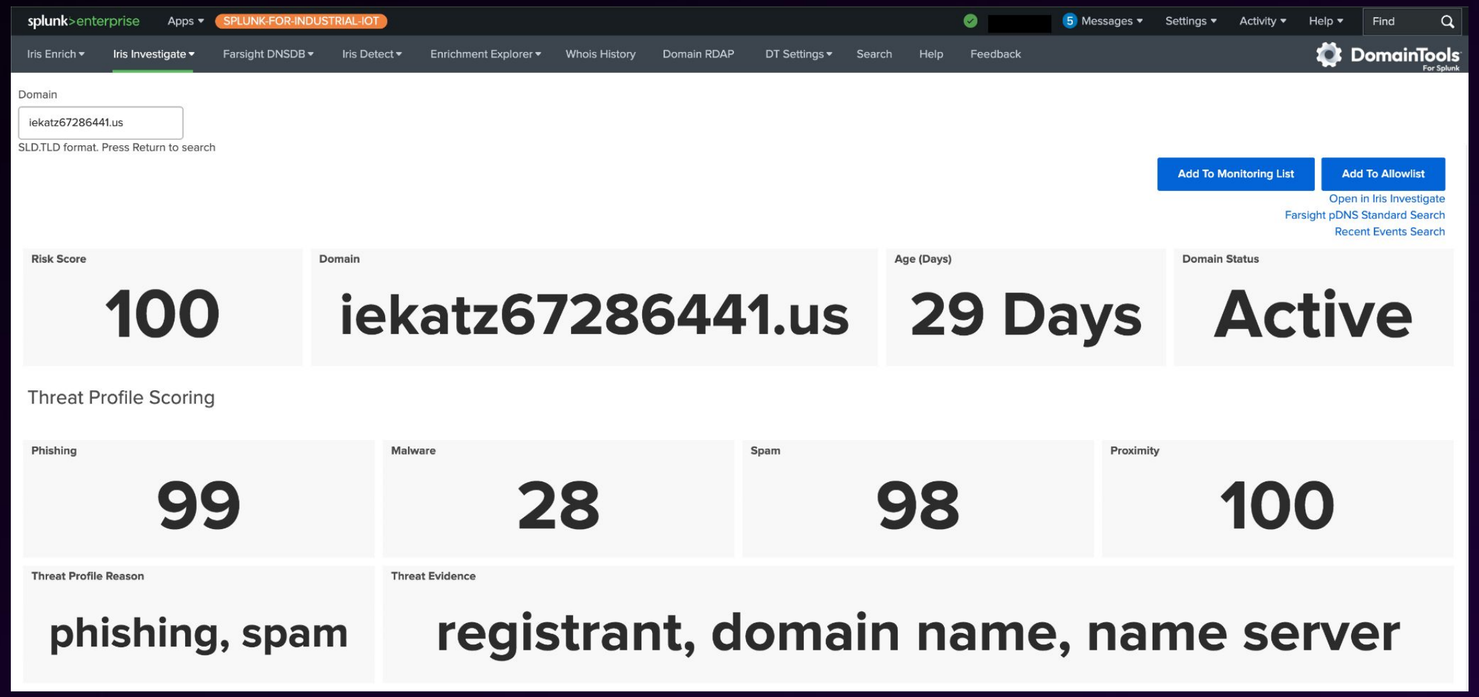
Attack Overview

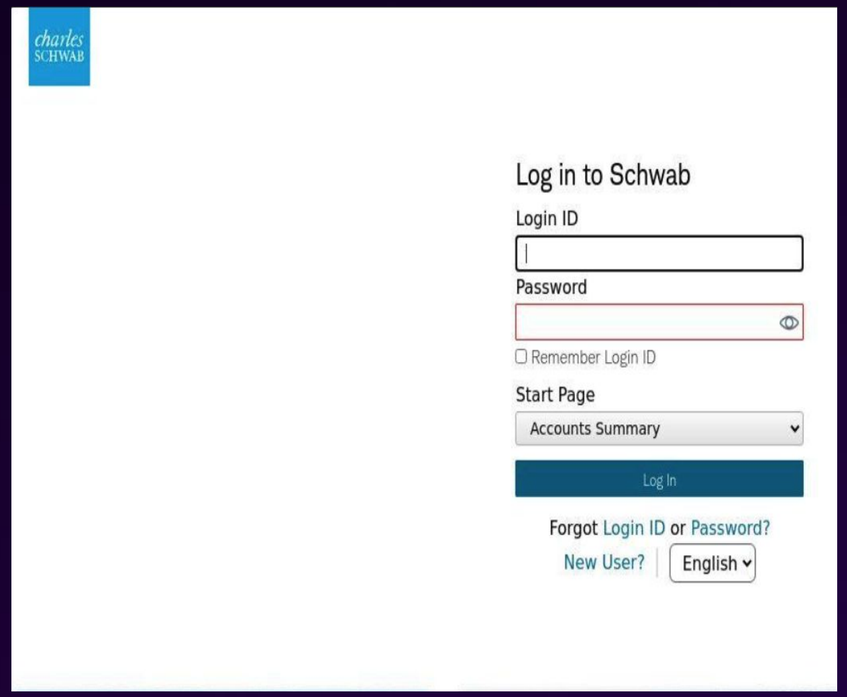
Initial Contact

- iPhone 14
- SW Ontario, CA area code
- Security notice for possible unexpected login attempt
- Subdomain
- Attributed to a TA named Chenlun/Sinkinto01



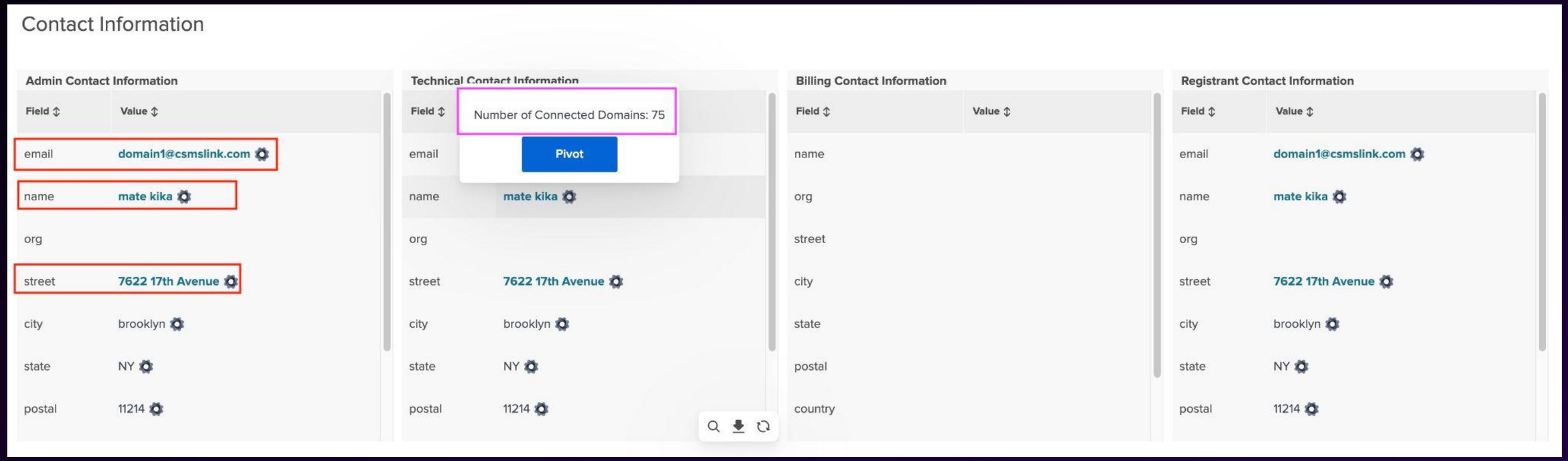
Domain Profile





- Domain is relatively young
- Shows high Domain Risk Score
- Charles Schwab login

Domain Profile



Guided Pivots:

- Alias tied to 75 other domains
- Email address
- Street address

DNS Activity

- Original subdomain seen 5/30/25
- Youngest subdomain seen 6/9/25
- Many other recently active subdomains

splunk>enterprise Apps SPLUNK-FOR-INDUSTRIAL-IOT

Iris Enrich | Iris Investigate | Farsight DNSDB | Iris Detect | Enrichment Explorer | Whois History | Domain RDAP | DT Settings | Search | Help | Fe

pDNS Standard Search

Farsight DNSDB Documentation

Time Range: All time

Resource Record Type (RRType): A

OR Add Custom RRTYPE: A

IP, Domain Name, FQDN or Subnet: *.iekatz67286441.us

Submit | Hide Filters

DNSDB RDATA Results

DNSDB RRSET Results

Time First	Time Last	RRName	RRType	bailiwick	RData
06/02/25 21:50:39	06/09/25 10:05:28	iekatz67286441.us.	A	iekatz67286441.us.	75.2.115.196
06/06/25 01:19:40	06/08/25 09:52:19	us46871hhguyez.iekatz67286441.us.	A	iekatz67286441.us.	75.2.115.196
06/06/25 13:52:42	06/08/25 02:18:26	www.us46871hhguyez.iekatz67286441.us.	A	iekatz67286441.us.	75.2.115.196
06/05/25 04:09:02	06/05/25 04:09:02	us43869xrr.iekatz67286441.us.	A	iekatz67286441.us.	75.2.115.196
06/02/25 22:58:41	06/04/25 03:53:53	www.iekatz67286441.us.	A	iekatz67286441.us.	75.2.115.196
06/02/25 22:07:42	06/03/25 14:21:24	us46871rctfy.iekatz67286441.us.	A	iekatz67286441.us.	75.2.115.196
05/30/25 10:22:41	06/02/25 11:01:49	iekatz67286441.us.	A	iekatz67286441.us.	104.21.16.69 172.67.166.226
05/30/25 18:51:01	05/30/25 18:51:01	us43869yoplfb.iekatz67286441.us.	A	iekatz67286441.us.	104.21.16.69 172.67.166.226

Related Domains

Pivoting on alias

19 other domains with same alias seen in the last month

Two patterns emerge. One at apex-level and another at the subdomain level

Domain	Risk Score
ajvsgx72941760.us	100
ccdwet22559668.us	100
ccrizv77518814.us	100
eyjveg50956366.us	100
iciqfv25486908.us	100
iekatz67286441.us	100
ieymob32761302.us	100
irbsoo67934556.us	100
ivecqk13344821.us	100
kiuddi95581479.us	100
kwmqpk84060386.us	100
nkqogc11466552.us	100
nqgopi95040498.us	100
renivj45317060.us	100
utnazq92814937.us	100
wjtvcn35599165.us	100
wpmcal14629035.us	100

Original domain has 5 subdomains

rrname
us43869xrr.iekatz67286441.us.
us43869fjjr.iekatz67286441.us.
us46871rctfy.iekatz67286441.us.
us43869bdgyfxl.iekatz67286441.us.
us46871hhguyez.iekatz67286441.us.

DGA Pattern

Example DGAs

randomstring20250718[.]com (date-based)

randomstring1752868754341[.]com (time-based)

abc12345[.]xyz (alphanumeric combo)

cityjulydish[.]net (word-based)

splunk>enterprise Apps SPLUNK-FOR-INDUSTRIAL-IOT

Iris Enrich Iris Investigate Farsight DNSDB Iris Detect Enrichment Explorer

pDNS Flexible Search

Flexible Search Documentation

Select a time range: All time

Query: ^us[[:digit:]]{5}.+\.[[:alpha:]]{6}[[:dig

Query type: RRName (Left-Hand)

rrname
us49951cxh.ajvsgx72941760.us.
us49951dvp.ajvsgx72941760.us.
us49951wzy.ajvsgx72941760.us.
us49951abej.ajvsgx72941760.us.
us49951dlqj.ajvsgx72941760.us.
us49951chfpf.ajvsgx72941760.us.
us49951wfeoq.ajvsgx72941760.us.
us49951lvmwrjm.ajvsgx72941760.us.
us43338cwa.ccdwet22559668.us.
us43338qkq.ccdwet22559668.us.

Regex Query Results

274 unique subdomains

```
^us[[:digit:]]{5}.+\.[[:alpha
:]]{6}[[:digit:]]{8}\.us\.$
```

Automating in Splunk

Demo

SPL Report

```
| dtdnsdbflex query_type=rrnames match_type=regex query="^us[[:digit:]]{5}.+\.[[:alpha:]]{6}[[:digit:]]{8}\.us\.$"
  time_last_after=`toEpoch("-24h@h")` time_first_before=`toEpoch("now")` rrtype="A"
| eval domain=lower(rrname)
| search NOT [ search index=chenlun_domains | stats values(domain) AS domain | table domain ]
| collect index=chenlun_domains marker="new_dns_entry"
| fields rrname rrtype
```

- Detect subdomains matching DGA pattern.
- Filter out domains already seen in past searches.
- Save the new subdomains for reference and analysis.
- Output the list of new, potentially malicious domains.

Demo

Scheduling the Report

- Set to run every 8hrs
- Priority can be raised depending on level of risk
- No schedule window for consistent execution

Edit Schedule

Report	Chenlun_Domain_Discovery
Schedule Report	☑ Learn More
Schedule	Run on Cron Schedule
Cron Expression	0 */8 * * *
Time Range	Last 24 hours
Schedule Priority ?	Default
Schedule Window ?	No window

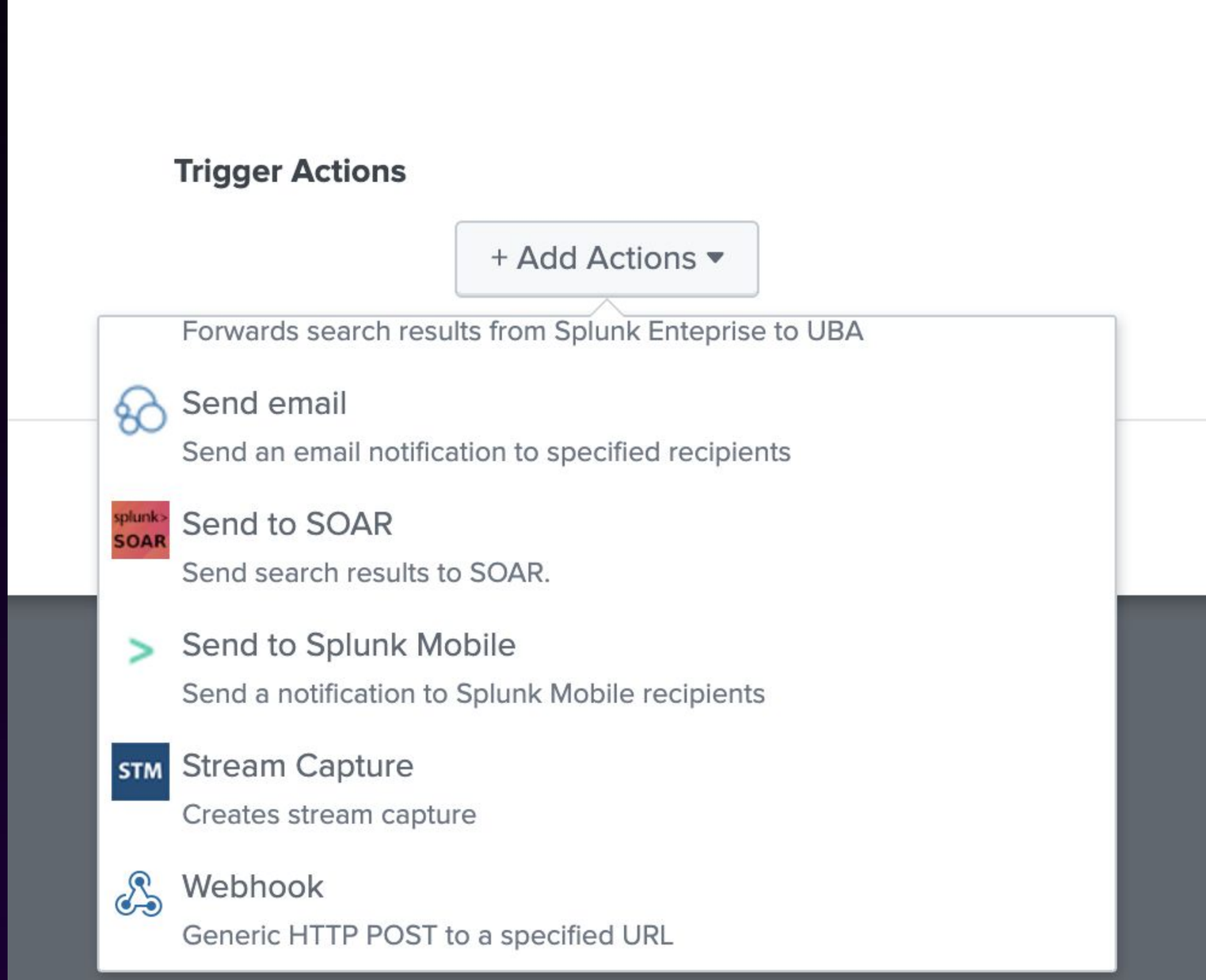
Trigger Actions

Demo

Trigger Actions

Automate an action after your report runs to:

- Email your SOC team
- Execute a custom script
- Trigger a Webhook
- Create a Notable Event
- Send results to Splunk SOAR

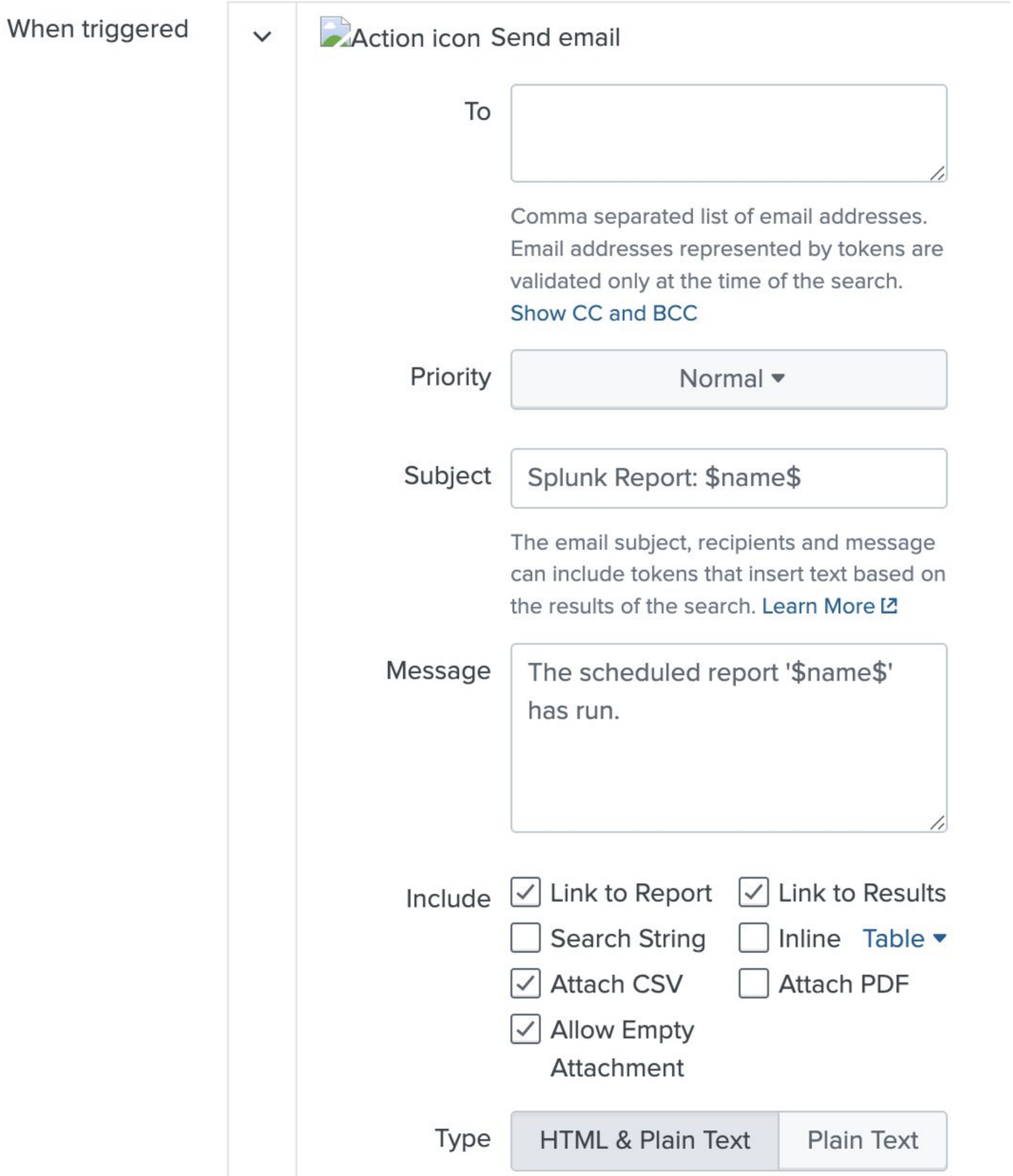


Last Mile Options

Email SOC Members

Send the latest results of the search via email:

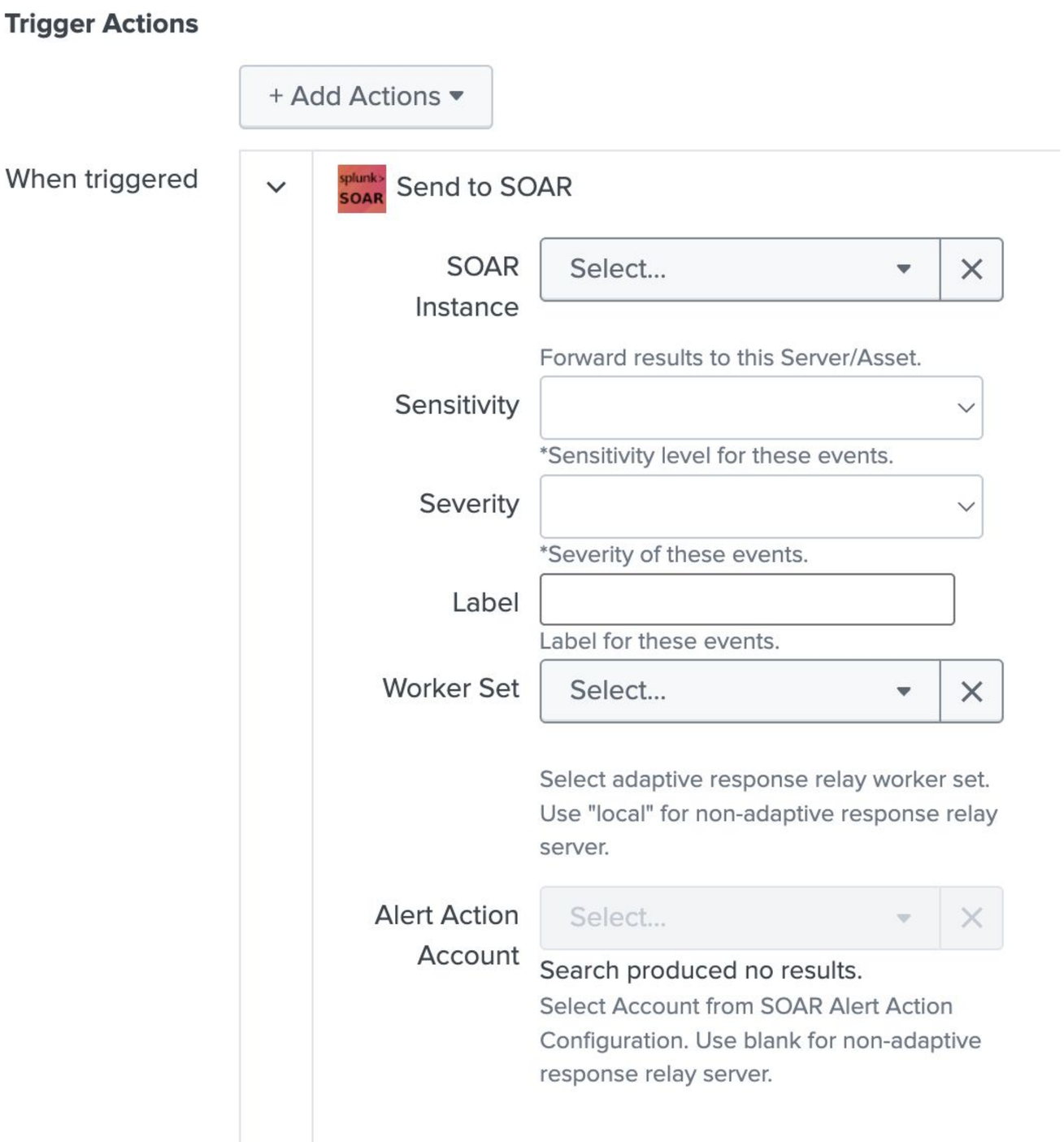
- Can include CSV of results
- Can link to the reports or results for easy access
- Adjust priority easily



Splunk SOAR

If you are a Splunk SOAR user, there are two handy options:

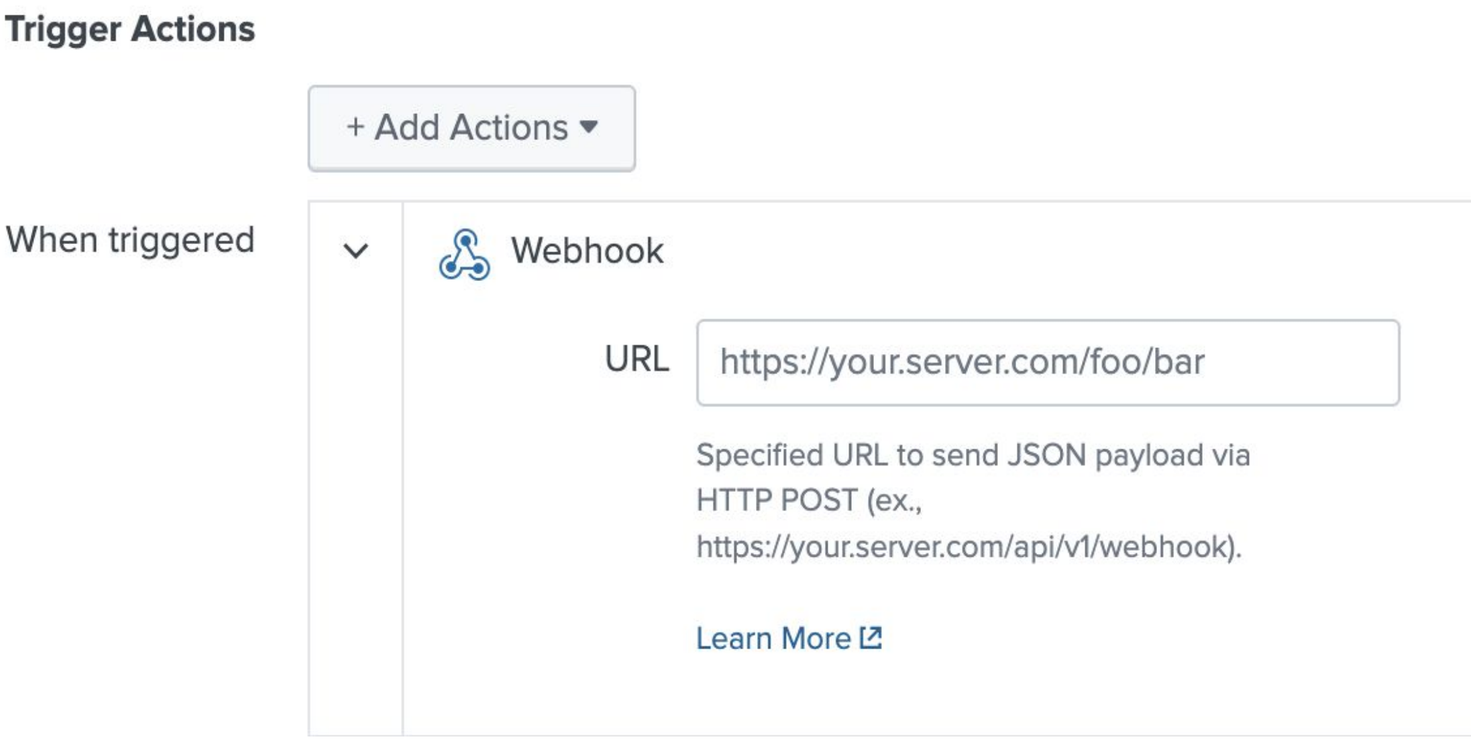
- Send to SOAR
- Run Playbook in SOAR



External SOAR

If you don’t use Splunk SOAR you can still use a trigger action to connect to your SOAR via:

- Webhook
- Custom Script



Sinkhole via DNS

If you know the results of your report are bad news and want to take immediate action by sinkholing at the DNS level.

```
$TTL 2h
@       IN      SOA     localhost. root.localhost. (
                        2025063001 ; serial
                        1h         ; refresh
                        15m        ; retry
                        30d        ; expire
                        2h )       ; minimum TTL

        IN      NS      localhost.

; Block specific domains by returning NXDOMAIN
bad-domain.com.         CNAME   .
malicious-site.net.     CNAME   .

; Redirect to a sinkhole IP
phishing-site.org.      A       192.0.2.1

; Wildcard block all subdomains
*.tracking-domain.com.  CNAME   .
```

Review

Single Domain

Pivot on data

DGA Pattern

Schedule Report

Trigger Actions

Possible Paths

Questions

Why do this?

1

Stay ahead of emerging threats

2

Reduce risk exposure

3

Improve team efficiency

Questions?

Thank You!

Steve
Behm

Solutions Engineer | Security Researcher
DomainTools
LinkedIn | email: sbehm@domaintools.com

.conf25
splunk>