SEC1336: Using Splunk to Catch Theft Rings

Taking Down Organized Retail Theft with DHCP Logs

Logan Foshee
Threat Intelligence Program Lead | Lowe's Companies

Nic Haag
Splunk PS Consultant | Aditum Partners

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

SEC1336: Using Splunk to Catch Theft Rings

Logan Foshee
Threat Intelligence Program Lead | Lowe's Companies

Nic Haag
Splunk PS Consultant | Aditum Partners

splunk> .conf19

"Retail theft costs U.S. companies **~$30 Billion** a year."

https://www.facefirst.com/blog/retail-loss-prevention-and-violent-crime-statistics/

"**Professional shoplifters** are responsible for 10% ($3B) of all retail theft. Averaging ~$800,000 for every $1b in sales, up **7% YOY**"

https://www.facefirst.com/blog/retail-loss-prevention-and-violent-crime-statistics/

https://www.retaildive.com/news/organized-retail-crime-continues-to-surge/543732/

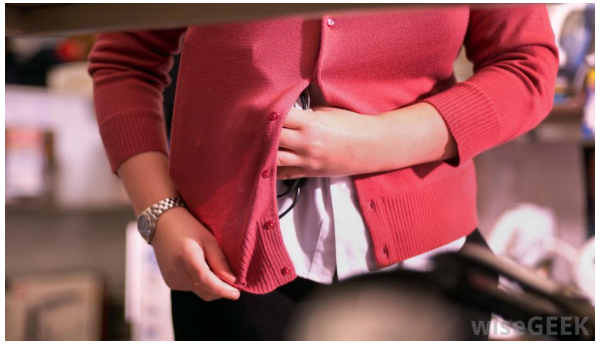
TTPs of Organized Theft

The different ways organized criminals make off the with goods

Push Cart

Fake Returns

Five-Finger Discount



How Can Splunk Help?

How do we stop or at least deter even some of this theft?

Questions that needed to be answered

- How to find out **who is in the store?**
- How do we **correlate known thefts to individuals?**
- How to **make complex data user friendly** for Loss Prevention investigators?

Most importantly: How do we **get results to the right people** that can take action ASAP?

Solved: Who is in the Store

The Magic Sauce: Instore Guest WiFi DHCP logs

```
index="infoblox" sourcetype="infoblox:dhcp" (dhcp_type=DHCPACK OR dhcp_type=DHCPREQUEST)
(( dest_ip=* [ | inputlookup StoreGuestWifiRange.csv | fields dest_ip ] ) OR
(src_ip=* [ | inputlookup StoreGuestWifiRange.csv | fields src_ip ] ))

| eval dest_mac=if(isnull(src_mac),dest_mac,src_mac)
| eval dest_ip=if(isnull(src_ip),dest_ip,src_ip)

| lookup CIDR2StoreNum.csv dest_ip OUTPUT StoreNumber
| lookup StoreNum2City.csv StoreNumber OUTPUT City, State/Province
| lookup CityLatLong.csv City, State/Province OUTPUT lat, long
| table dest_mac, dest_ip, City, State/Province, StoreNumber, lat, long
```

Solved: Correlating Known Thefts to Individuals

Step 1: Finding A Common Bad Actor

Input 1st Store # | Month | Day

12345 | August | 1

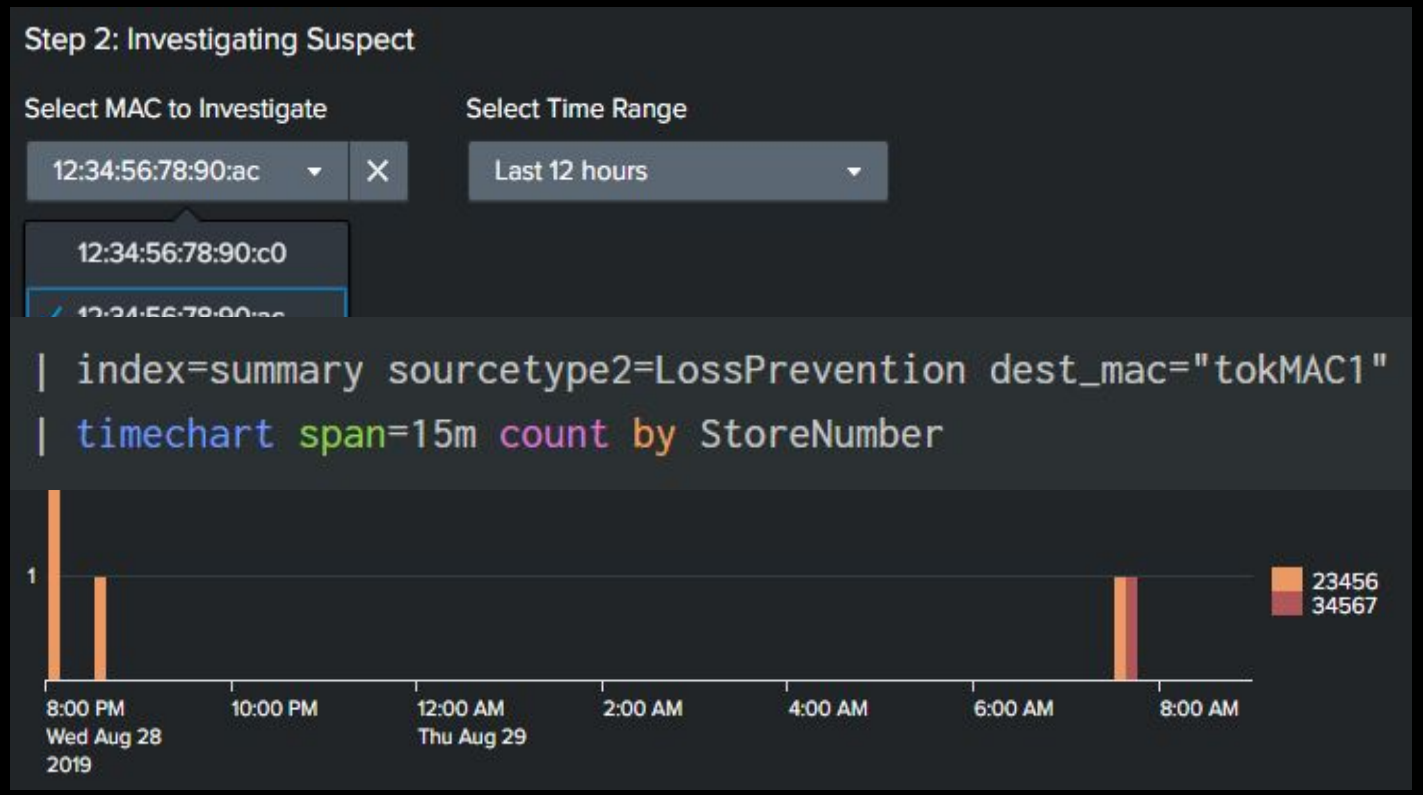
```
index=summary sourcetype2=LossPrevention
(StoreNumber=$tokSN1$ date_month=$tokM1$ date_mday=$tokD1$) OR
(StoreNumber=$tokSN2$ date_month=$tokM2$ date_mday=$tokD2$) OR
(StoreNumber=$tokSN3$ date_month=$tokM3$ date_mday=$tokD3$)
| stats dc(StoreNumber) by dest_mac
| rename dc(StoreNumber) as Store_Hits
| where Store_Hits > 1
| sort -Store_Hits
```

12:34:56:78:90:ac	2
12:34:56:78:90:ad	2
12:34:56:78:90:af	2

An analyst inputs dates and stores of known thefts believed to be linked to same Master Case.

The goal being to isolate a MAC address that was present during multiple events.

Solved: Complex Data Made User Friendly



We can further refine by time, to provide within an approximate time window of when the individual entered and left the store.

Loss Prevention Dashboard

Edit | Export | ...

Step 1: Finding A Common Bad Actor

Input 1st Store #	Month	Day
12345	August	1

Input 2nd Store #	Month	Day
23456	September	2

Input 3rd Store #	Month	Day
34567	October	3

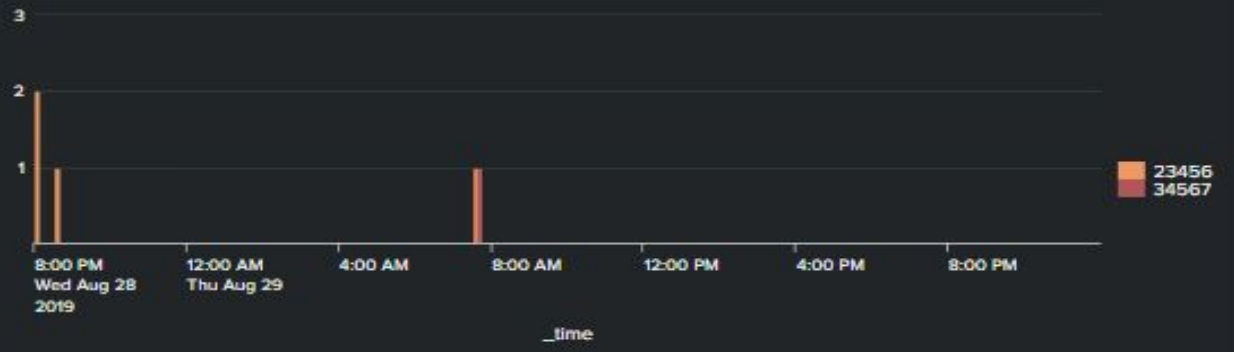
dest_mac	Store_Hits
12:34:56:78:90:c0	4
12:34:56:78:90:ac	2
12:34:56:78:90:ad	2
12:34:56:78:90:af	2

Step 2: Investigating Suspect

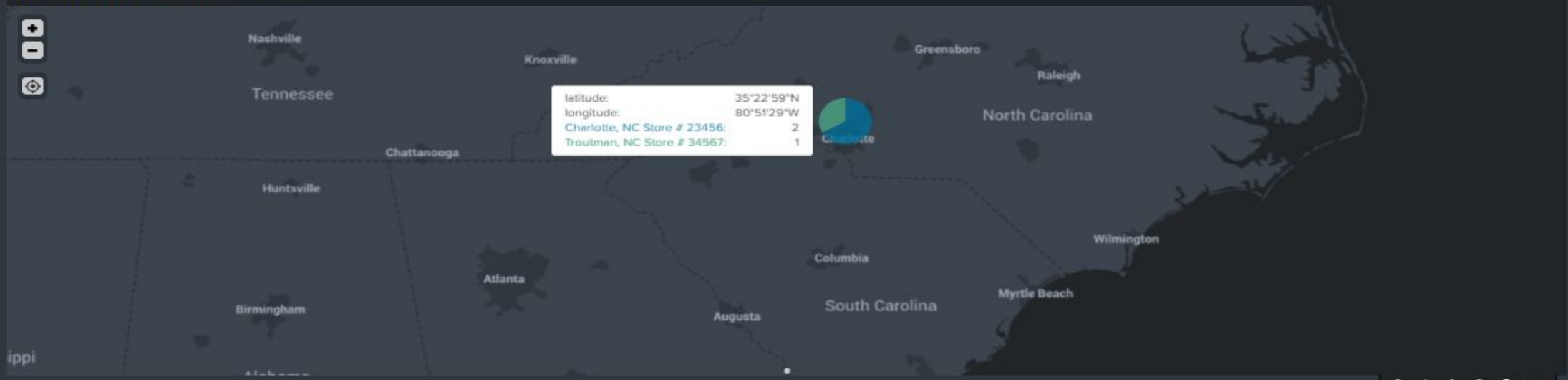
Select MAC to Investigate: 12:34:56:78:90:ac

Select Time Range: Custom time

Time In Store



Locations for 12:34:56:78:90:ac



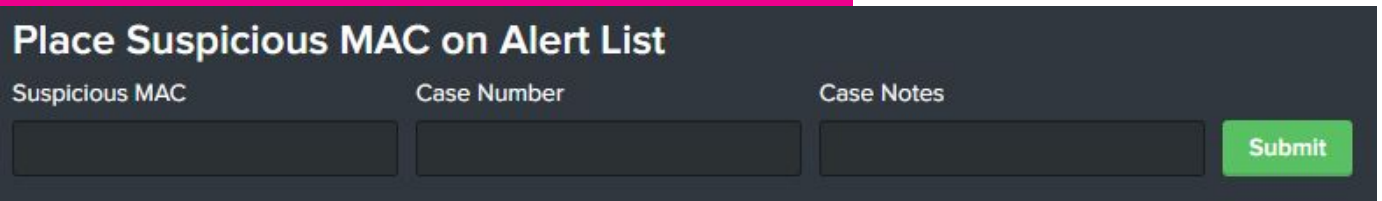
6m ago

You're on the List

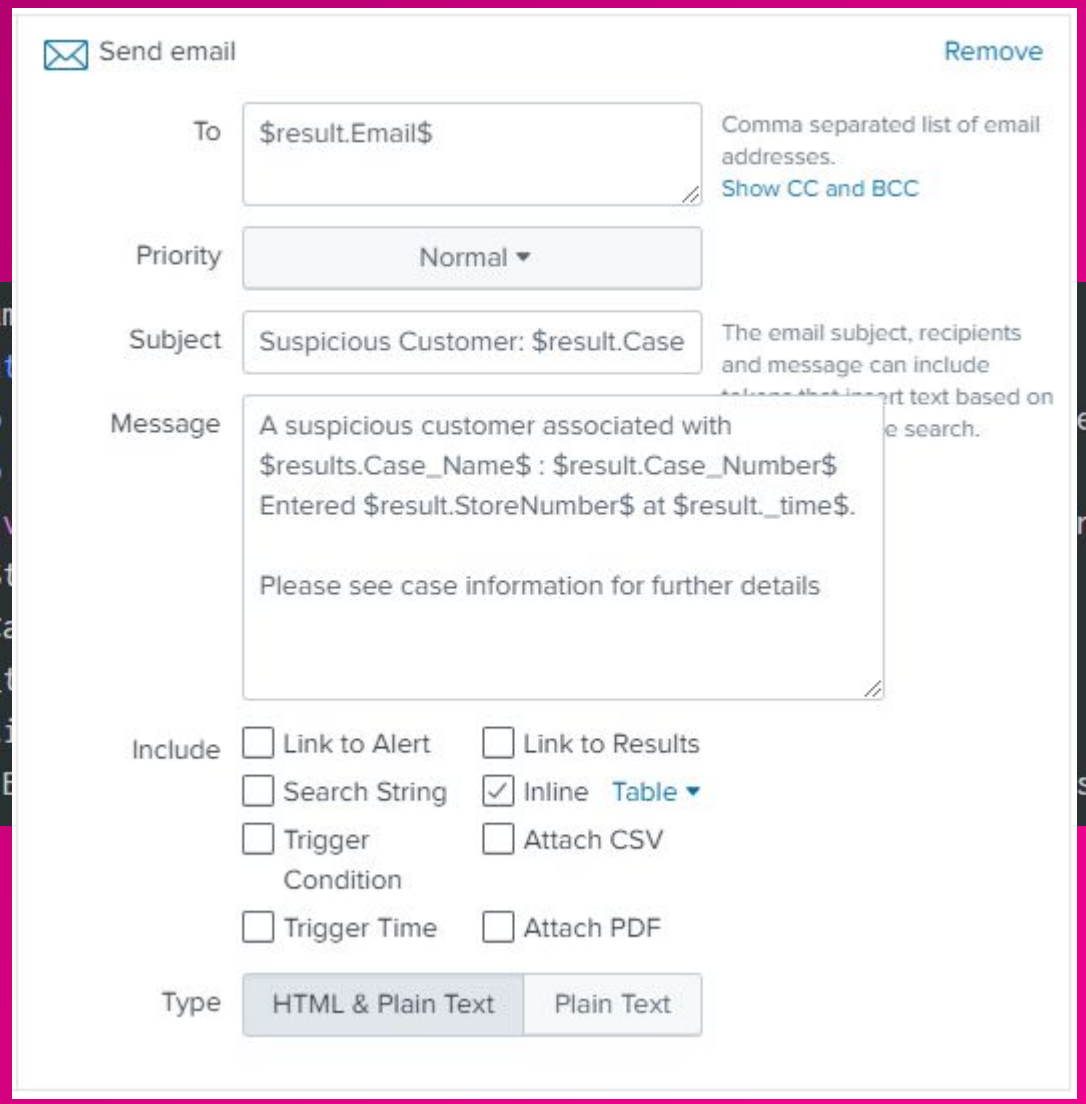
Populating a Lookup from an input panel

1. Once a device has been found present at an unusually high number of known thefts, it goes on the list.

2. This input panel allows an investigator to flag a MAC address is suspicious, as well as add relevant case information

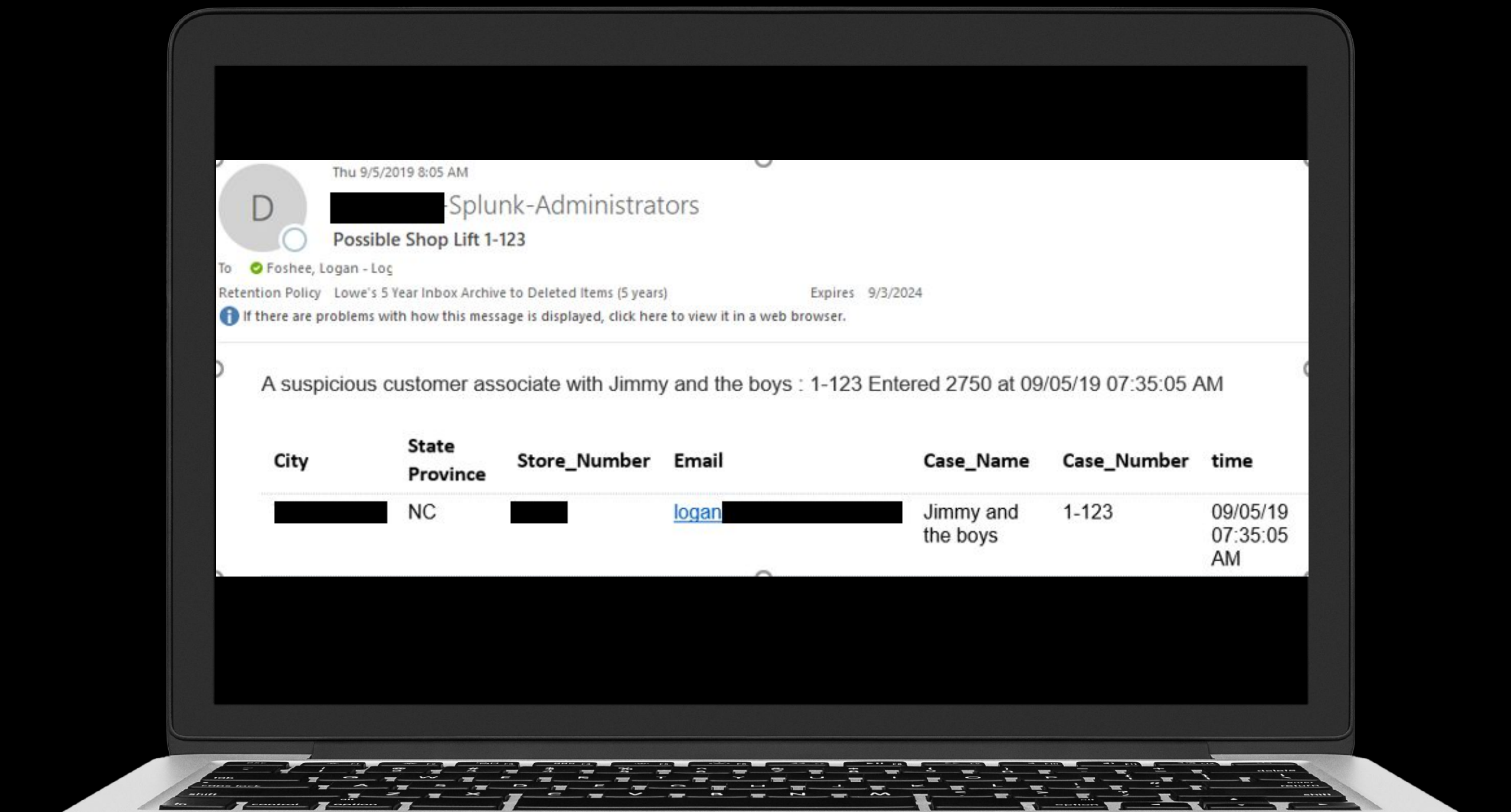


Solved: Getting results to the right people



With an alerting running every 5m, we can compare our suspicious MAC list, to MACs currently active in the stores

By tokenizing the email alert action, and leveraging stats ‘values’ we can ensure emails are only sent to the relevant people.


Thu 9/5/2019 8:05 AM
D
[redacted]-Splunk-Administrators
Possible Shop Lift 1-123
To Foshee, Logan - Log
Retention Policy Lowe's 5 Year Inbox Archive to Deleted Items (5 years) Expires 9/3/2024
If there are problems with how this message is displayed, click here to view it in a web browser.
A suspicious customer associate with Jimmy and the boys : 1-123 Entered 2750 at 09/05/19 07:35:05 AM
City
State Province
Store_Number
Email
Case_Name
Case_Number
time
[redacted]
NC
[redacted]
logan[redacted]
Jimmy and the boys
1-123
09/05/19 07:35:05 AM

Summary

Using Splunk to Catch Theft Rings

Grabbing Near-Real time DHCP data

Correlating Against Open Cases

Identifying Bad Actors

Proactive alerting on Bad Actors

Future Growth

Where we plan to take this use case going forward

1. Integrating the LP database with Splunk
2. Proactive Theft ”Hunting”
3. Harnessing DHCPDISCOVERY Events

.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION