Profiling Encrypted Network Traffic

splunk> .conf19

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.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

Profiling Encrypted Network Traffic

Jayson Weiss

Security Engineer III at Box

Mike Sconzo

Staff Threat Intel Engineer

Visibility. Is. Crucial.

Activity Profiles

What should you be looking for in encrypted network traffic

Benign

- Keep sensitive data secure (e.g. web sessions, email, data transactions)

Malicious

- C2/Data exfiltration
- Hiding of exploit delivery
- Phishing email delivery/reception

Policy

- Sites/activity that aren't malicious, but pose risk to the business (HR, etc...)

Unknown

- Fertile hunting grounds

Technology Overview

#TechGoals

splunk> .conf19

Data

Choose your own adventure

Process Data

- Executable that spawned the process
- IPs/hosts the process is connecting to
- Hash of the executable

Network Data

- Source/destination IPs
- Monitor SSL/encrypted traffic

Signatures for Matching

- Need to consolidate protocol properties to an easily defined signature

Process Data

Carbon Black

Behavioral detection

- Detects applications doing things like scraping memory, key logging, spawning shells, etc

Process and binary search of centralized data

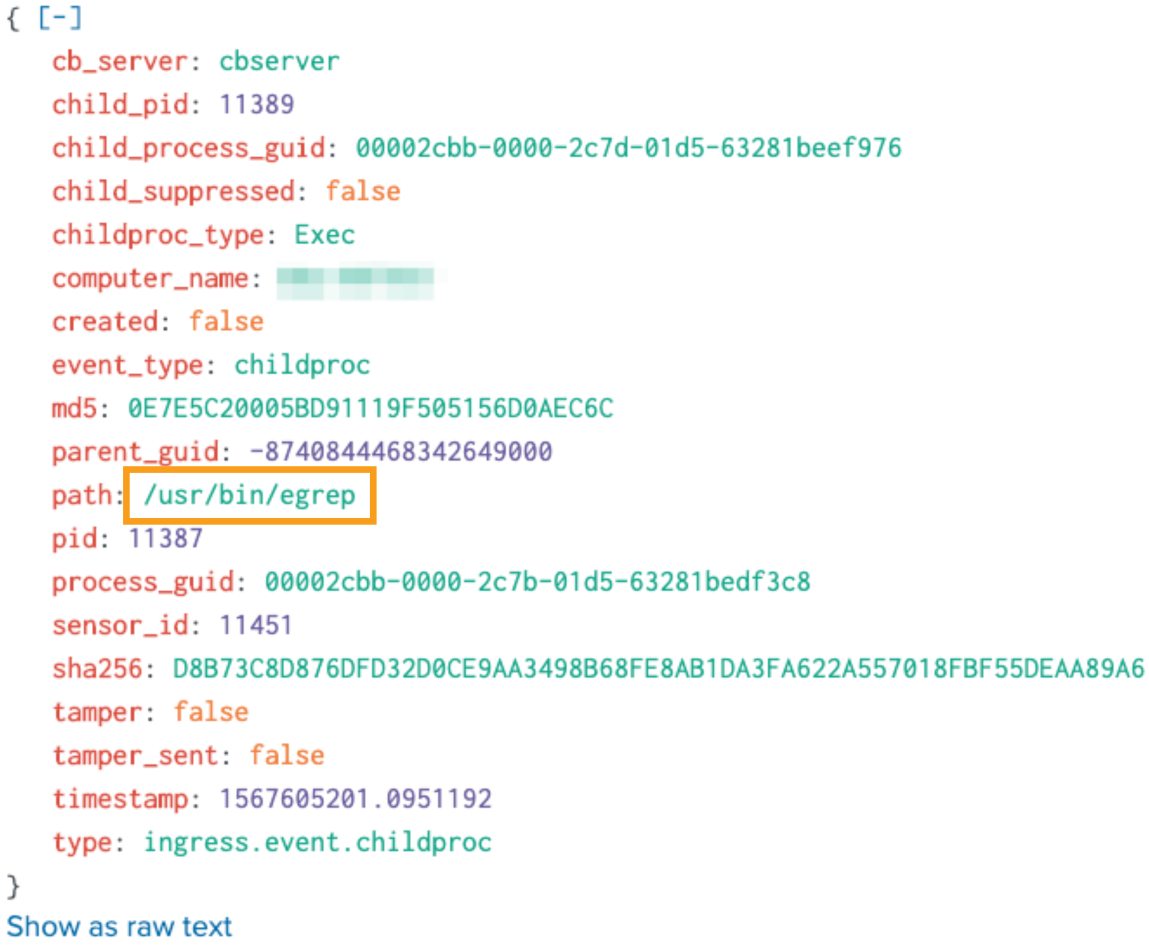
- Hash and behavior based

Process based network activity

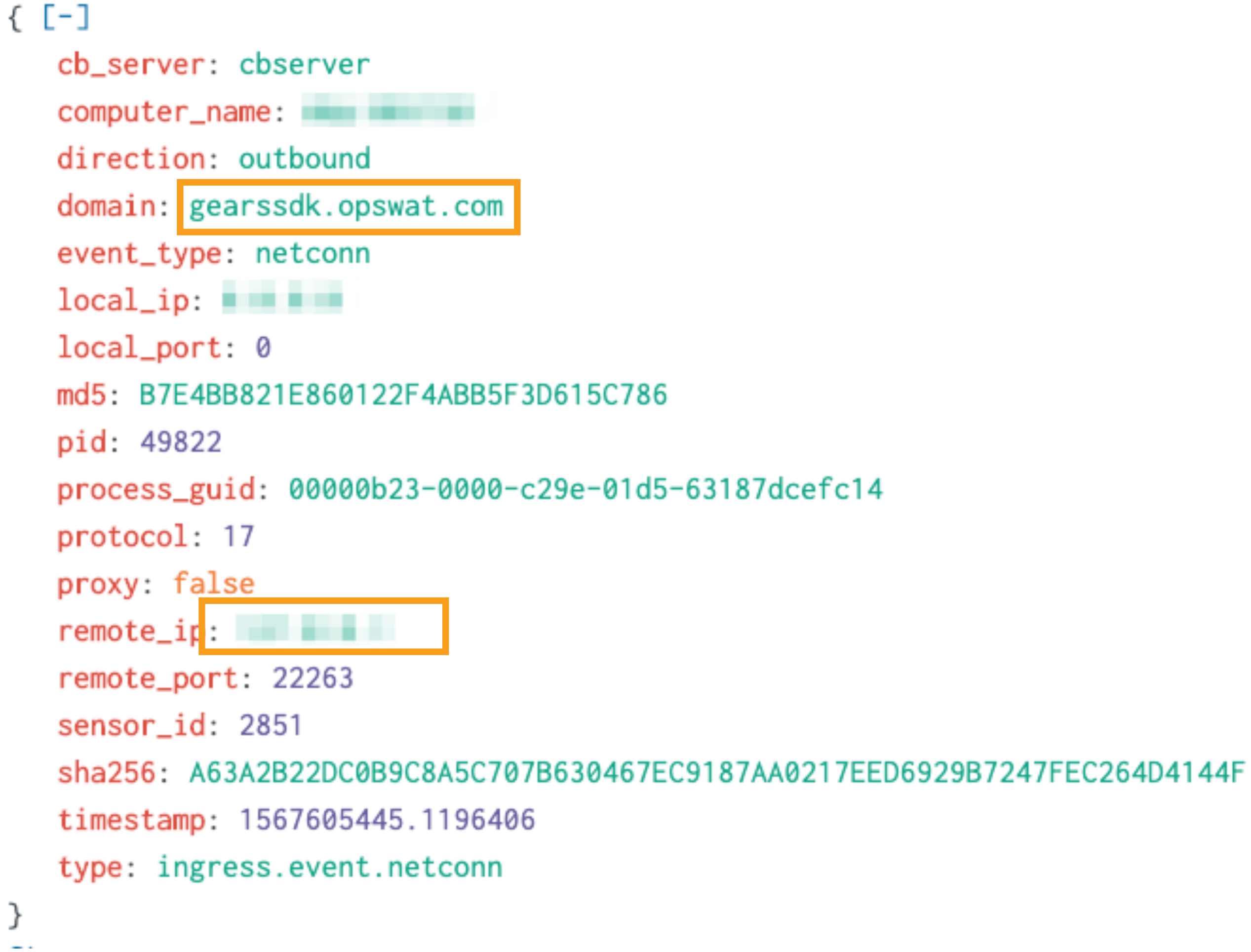
Live Response remediation

- Allows for host isolation
- Allows you to have a terminal shell on the host to kill process, add or delete files, perform mem dumps, etc

Carbon Black Data



```
{ [-]
   cb_server: cbserver
   child_pid: 11389
   child_process_guid: 00002cbb-0000-2c7d-01d5-63281beef976
   child_suppressed: false
   childproc_type: Exec
   computer_name: [redacted]
   created: false
   event_type: childproc
   md5: 0E7E5C20005BD91119F505156D0AEC6C
   parent_guid: -8740844468342649000
   path: /usr/bin/egrep
   pid: 11387
   process_guid: 00002cbb-0000-2c7b-01d5-63281bedf3c8
   sensor_id: 11451
   sha256: D8B73C8D876DFD32D0CE9AA3498B68FE8AB1DA3FA622A557018FBF55DEAA89A6
   tamper: false
   tamper_sent: false
   timestamp: 1567605201.0951192
   type: ingress.event.childproc
}
Show as raw text
```



```
{ [-]
   cb_server: cbserver
   computer_name: [redacted]
   direction: outbound
   domain: gearssdk.opswat.com
   event_type: netconn
   local_ip: [redacted]
   local_port: 0
   md5: B7E4BB821E860122F4ABB5F3D615C786
   pid: 49822
   process_guid: 00000b23-0000-c29e-01d5-63187dcefc14
   protocol: 17
   proxy: false
   remote_ip: [redacted]
   remote_port: 22263
   sensor_id: 2851
   sha256: A63A2B22DC0B9C8A5C707B630467EC9187AA0217EED6929B7247FEC264D4144F
   timestamp: 1567605445.1196406
   type: ingress.event.netconn
}
```

Network Activity

Zeek (formerly Bro)

Open Source Network Monitoring tool

Passive IDS

- Can leverage various types of signatures

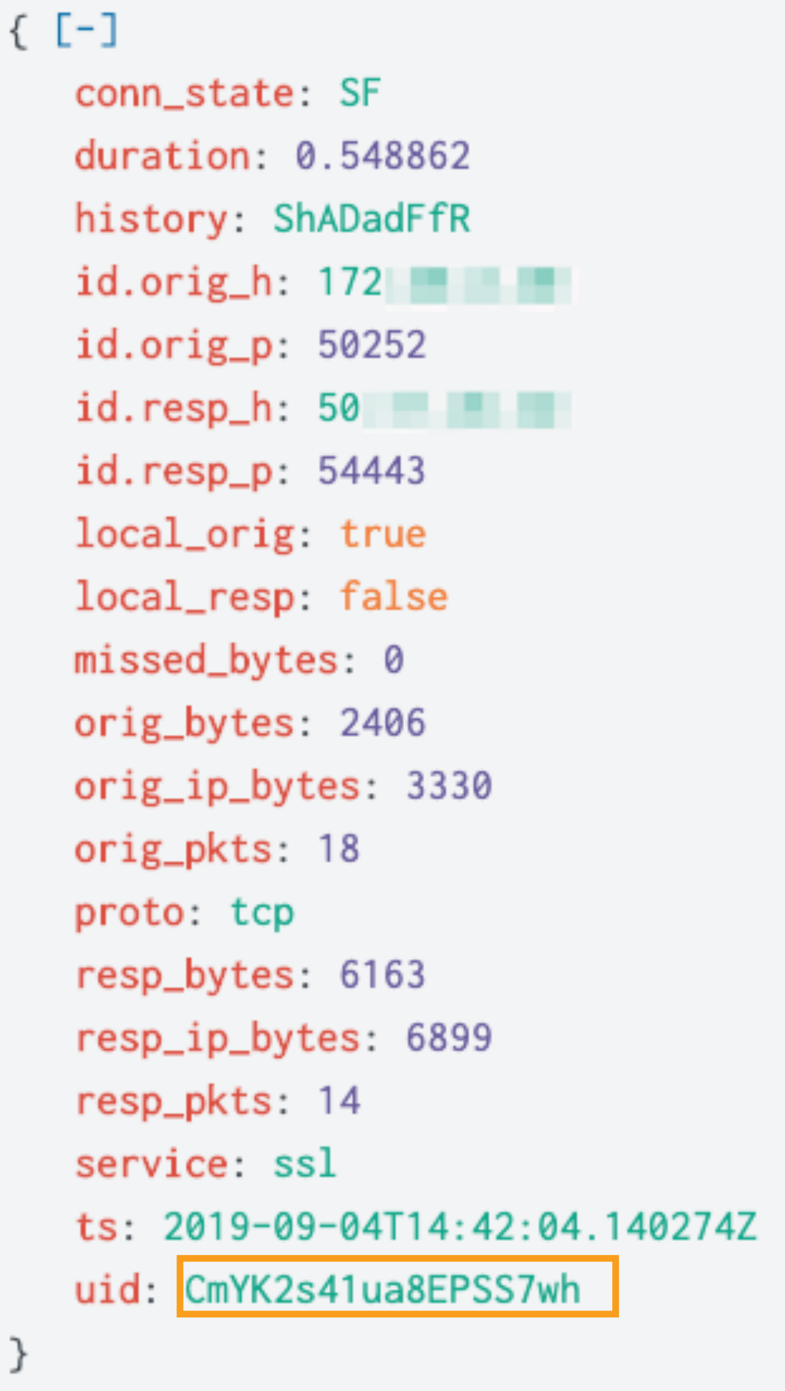
Scriptable

- Extend network monitoring capability

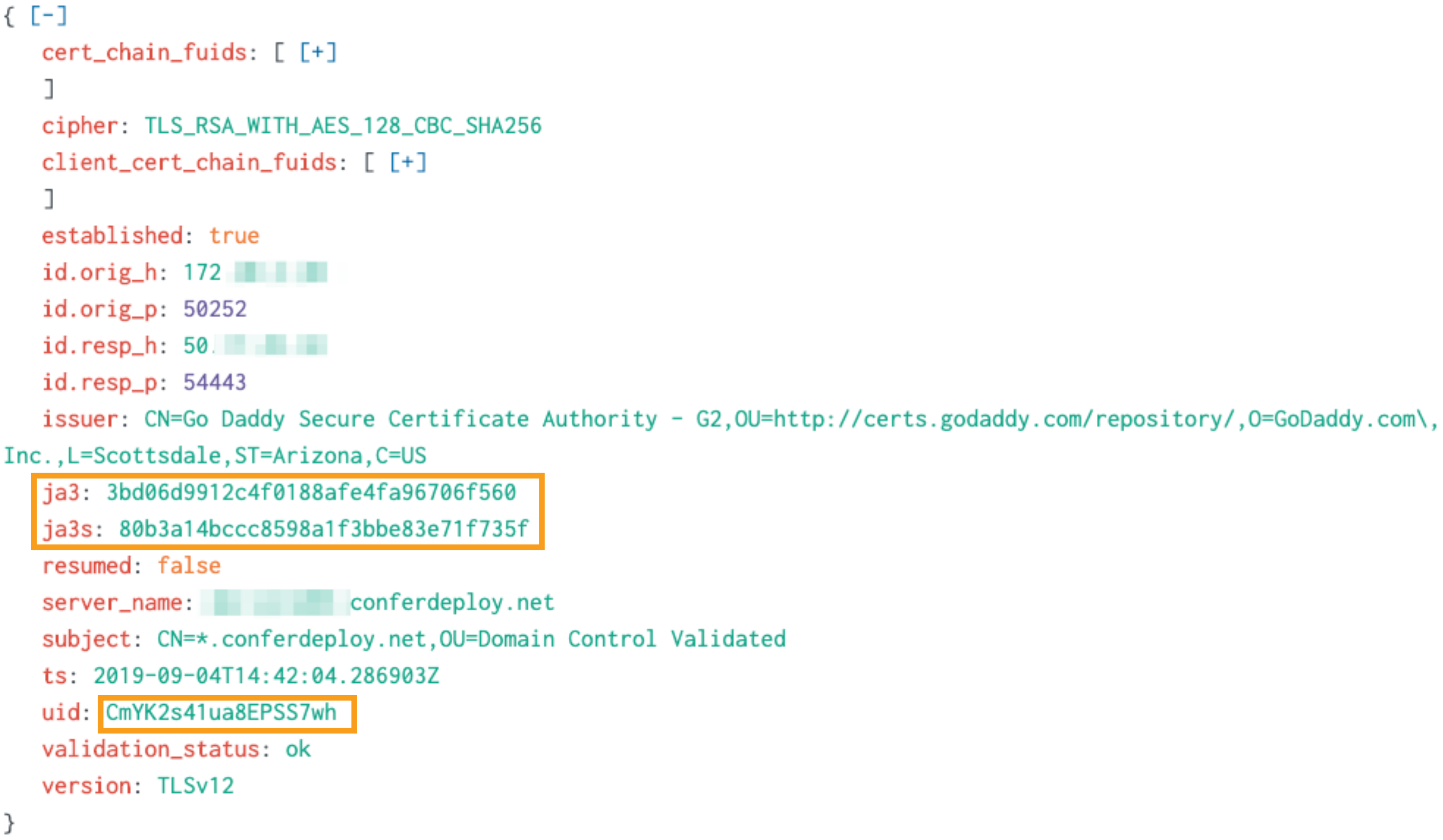
Logs everything that it sees allowing for forensics

- Common protocols: HTTP, SSL, SMTP, SSH, etc…
- Logs can be sent to Splunk

Zeek Data



```
{ [-]
   conn_state: SF
   duration: 0.548862
   history: ShADadFfR
   id.orig_h: 172[redacted]
   id.orig_p: 50252
   id.resp_h: 50[redacted]
   id.resp_p: 54443
   local_orig: true
   local_resp: false
   missed_bytes: 0
   orig_bytes: 2406
   orig_ip_bytes: 3330
   orig_pkts: 18
   proto: tcp
   resp_bytes: 6163
   resp_ip_bytes: 6899
   resp_pkts: 14
   service: ssl
   ts: 2019-09-04T14:42:04.140274Z
   uid: CmYK2s41ua8EPSS7wh
}
```



```
{ [-]
   cert_chain_fuids: [ [+]
   ]
   cipher: TLS_RSA_WITH_AES_128_CBC_SHA256
   client_cert_chain_fuids: [ [+]
   ]
   established: true
   id.orig_h: 172 [redacted]
   id.orig_p: 50252
   id.resp_h: 50.[redacted]
   id.resp_p: 54443
   issuer: CN=Go Daddy Secure Certificate Authority - G2,OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\,
Inc.,L=Scottsdale,ST=Arizona,C=US
   ja3: 3bd06d9912c4f0188afe4fa96706f560
   ja3s: 80b3a14bccc8598a1f3bbe83e71f735f
   resumed: false
   server_name: [redacted]conferdeploy.net
   subject: CN=*.conferdeploy.net,OU=Domain Control Validated
   ts: 2019-09-04T14:42:04.286903Z
   uid: CmYK2s41ua8EPSS7wh
   validation_status: ok
   version: TLSv12
}
```

splunk>

Making machine data accessible, usable and valuable to everyone.

Networking

How the packets work

LEFT
EXIT 12
COOL SPL
BASICS AND LEVEL SETTING
US
imgflip.com

SSL

What is it?

Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client.

Uses certificates issued by a trusted CA

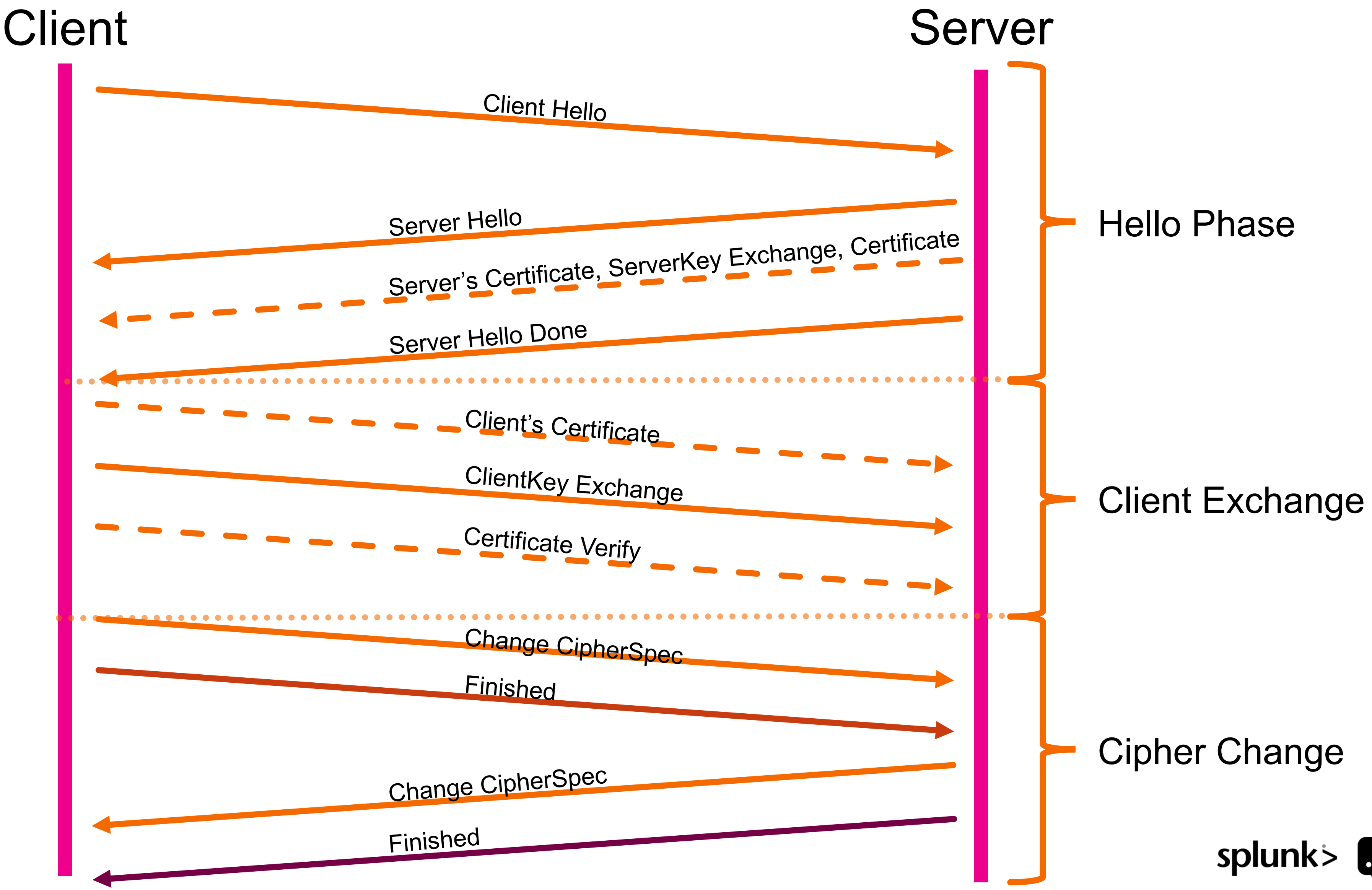
- Uses a public private key pair to establish an encrypted connection

Allows for the secure transfer of sensitive information

Used over TCP

SSL

Setup/Negotiation



JA3

What is JA3?

JA3 is a method of fingerprinting SSL/TLS encrypted network traffic. This allows you to identify what is on your network, establish a baseline and alert on anomalous activity

Developed around Lee Brotherston's 2015 research

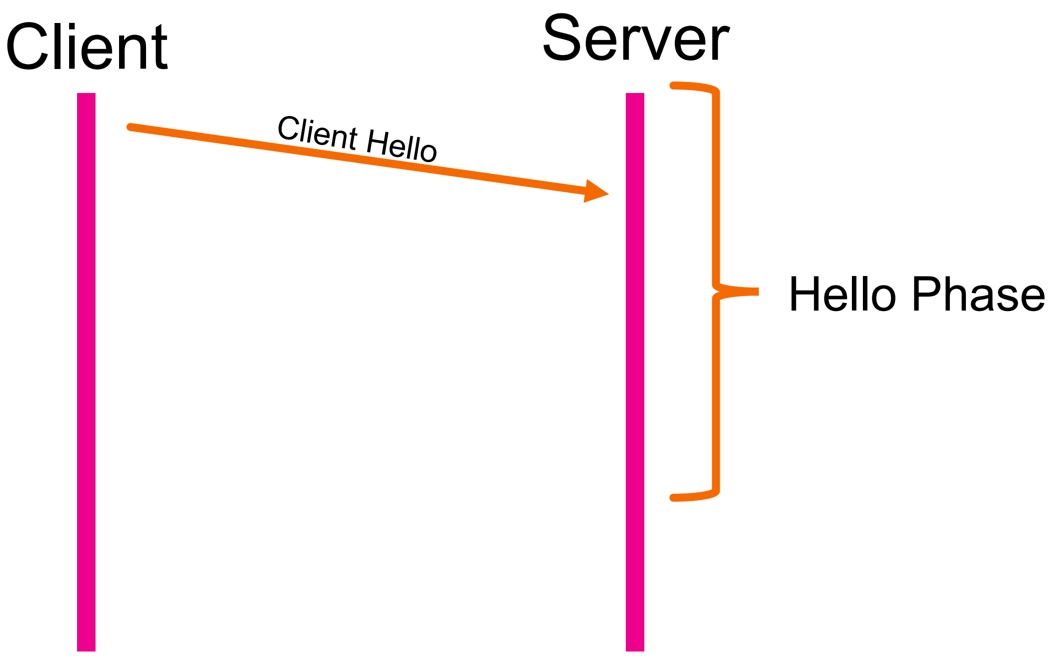
- Lee's DerbyCon talk: https://www.youtube.com/watch?v=XX0FRAy2Mec

Allows you to identify what's on your network and establish a baseline

- Identifies potentially malicious activity without having to MITM your encrypted network traffic
- Resource: https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967

JA3

How it works



```
▼ TLSv1 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 158
  ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 154
      Version: TLS 1.0 (0x0301)
    ▶ Random: 50839cfafec110ae58d1edc2f2ffc51ec3c2e7ca65221bd4...
      Session ID Length: 0
      Cipher Suites Length: 72
    ▼ Cipher Suites (36 suites)
        Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
                 ...
      Compression Methods Length: 1
    ▶ Compression Methods (1 method)
      Extensions Length: 41
    ▶ Extension: server_name (len=15)
    ▶ Extension: supported_groups (len=8)
    ▼ Extension: ec_point_formats (len=2)
        Type: ec_point_formats (11)
        Length: 2
        EC point formats Length: 1
      ▼ Elliptic curves point formats (1)
          EC point format: uncompressed (0)
    ▶ Extension: SessionTicket TLS (len=0)
```

769,255-49160-49172-...51-50-49164,,0

=

86ed02e0de5a31b81cc0cd8484f90d0f

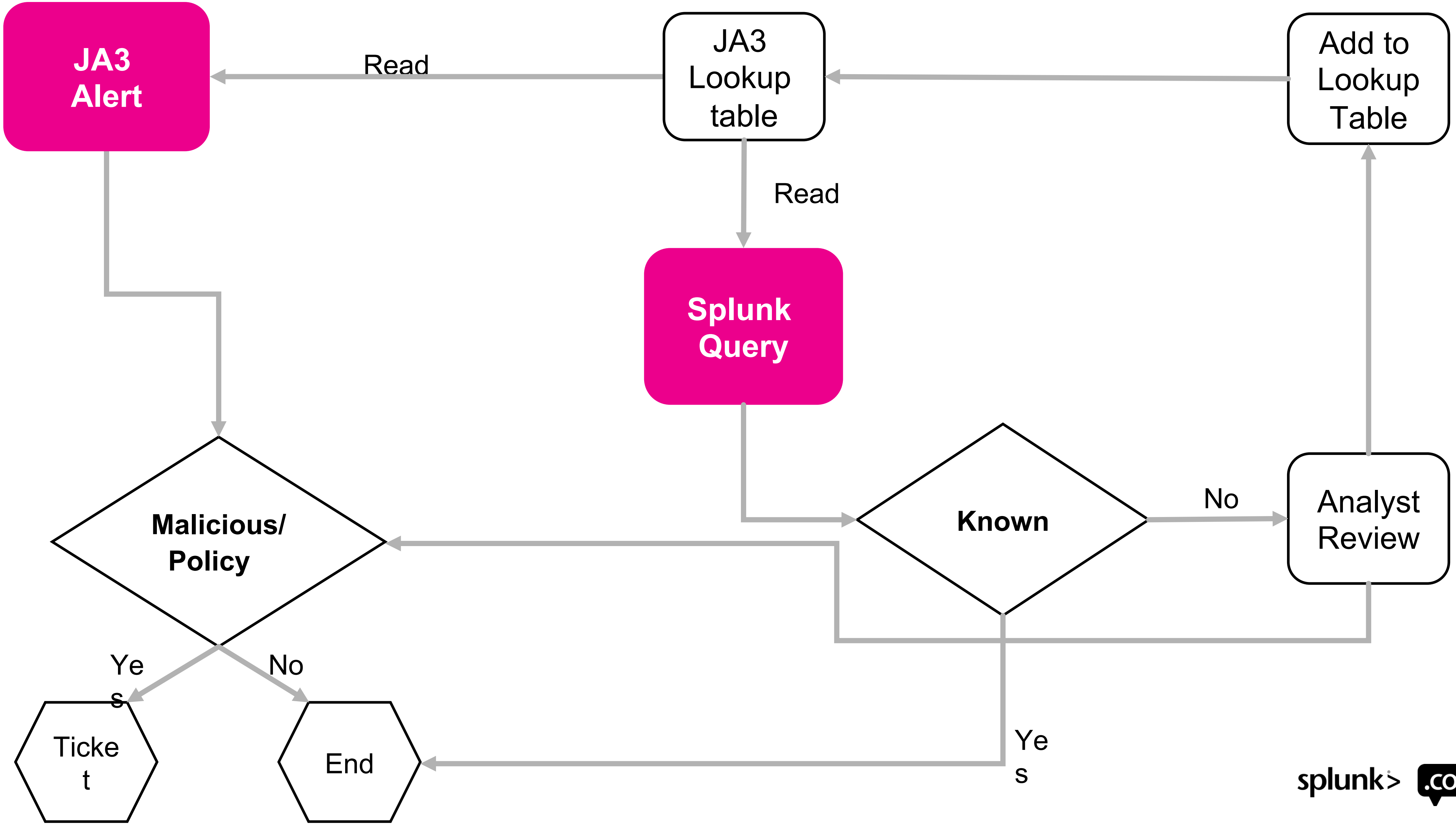
Solution

Tying it all together

Phase 1

JA3

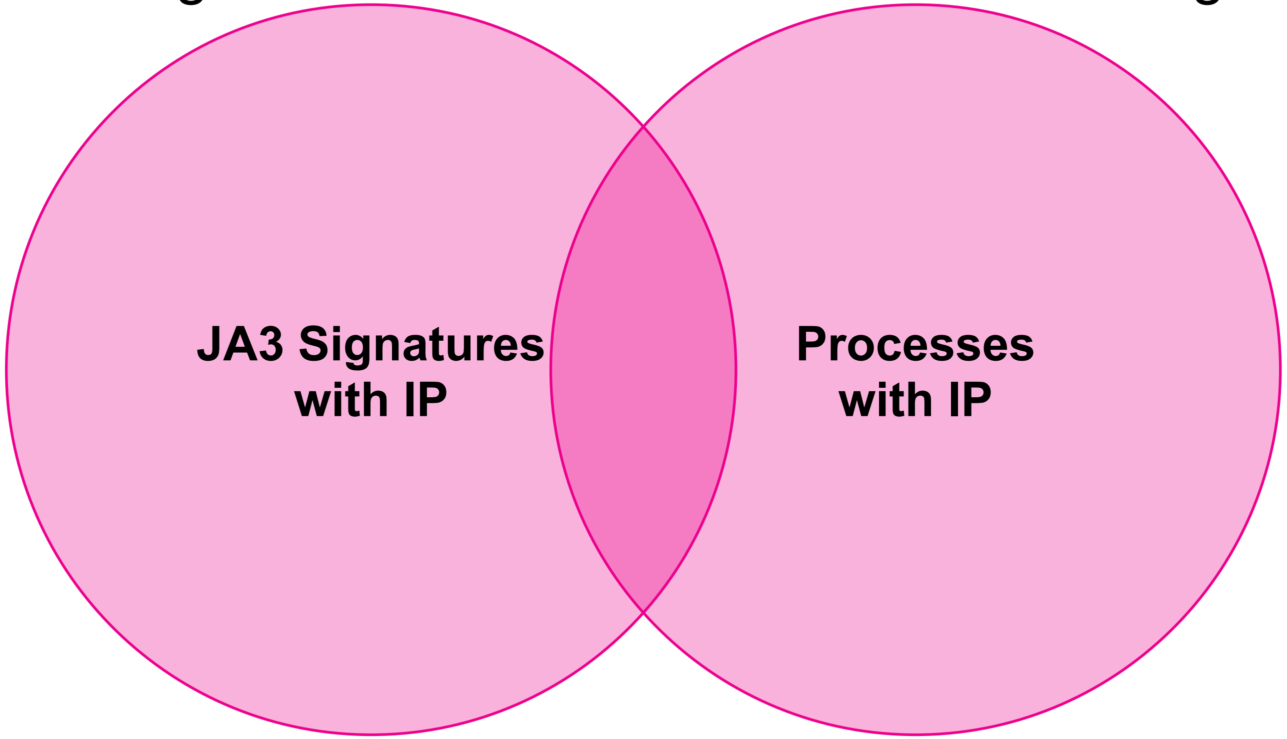
Workflow


JA3 Alert
Read
JA3 Lookup table
Add to Lookup Table
Read
Splunk Query
Malicious/ Policy
Known
No
Analyst Review
Ye
s
No
Ticke
t
End
Ye
s

Round 1

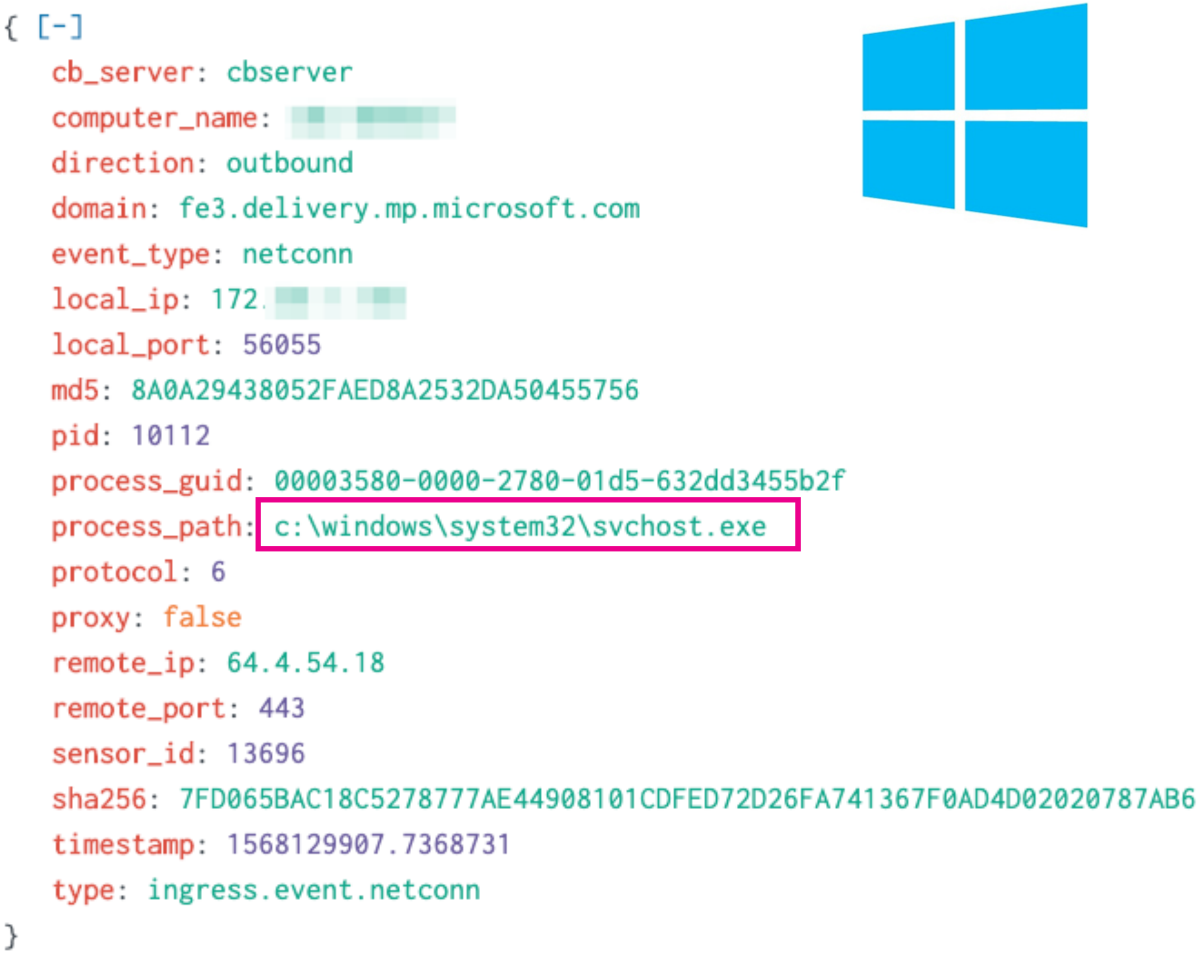
"JOIN"

Coming from an SQL background and Inner Join seemed like the right solution.

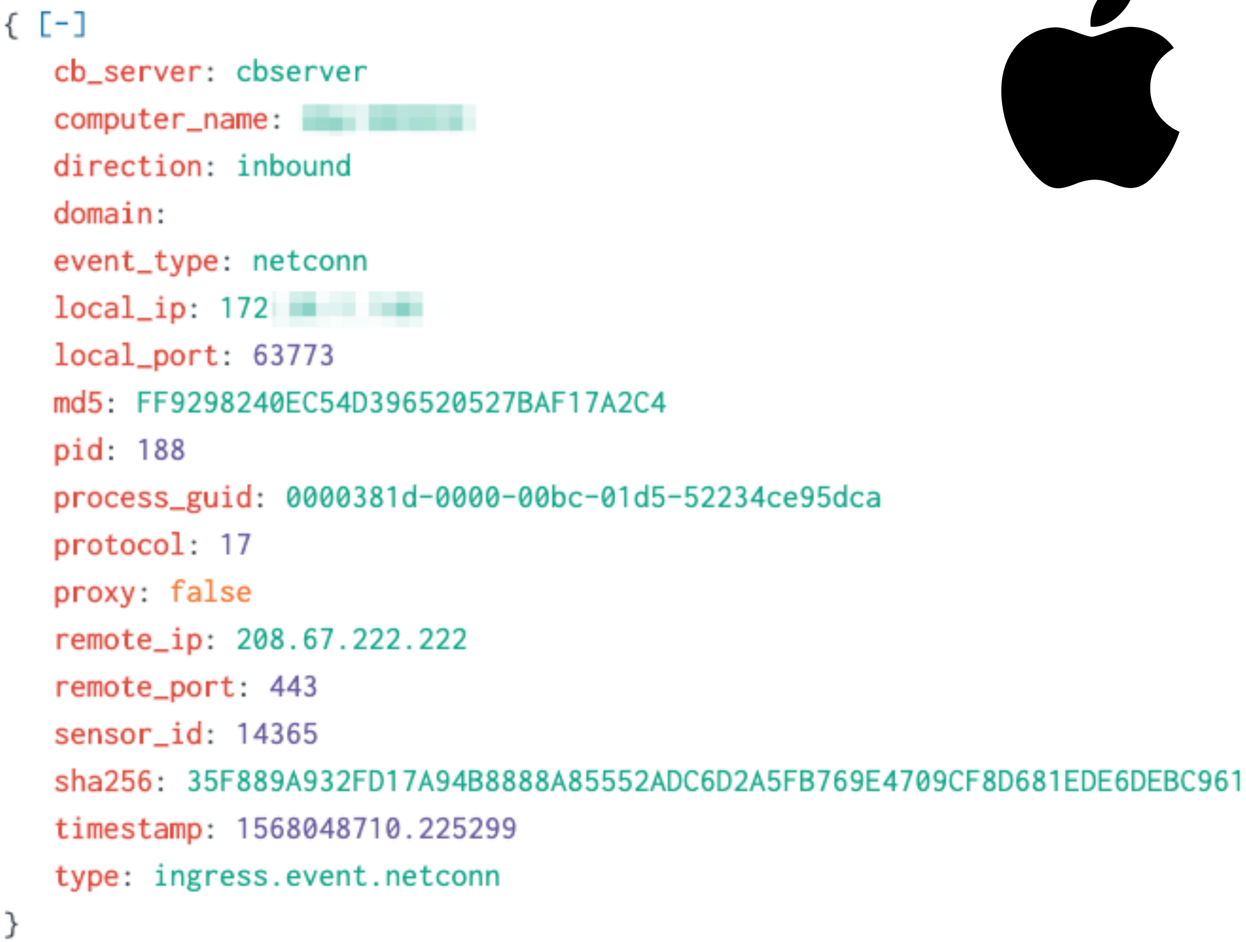


Splunk
Our "good" ideas
PACQUIAO
CAFÉ PURO
RICOA
GCOX

Problems with the Data

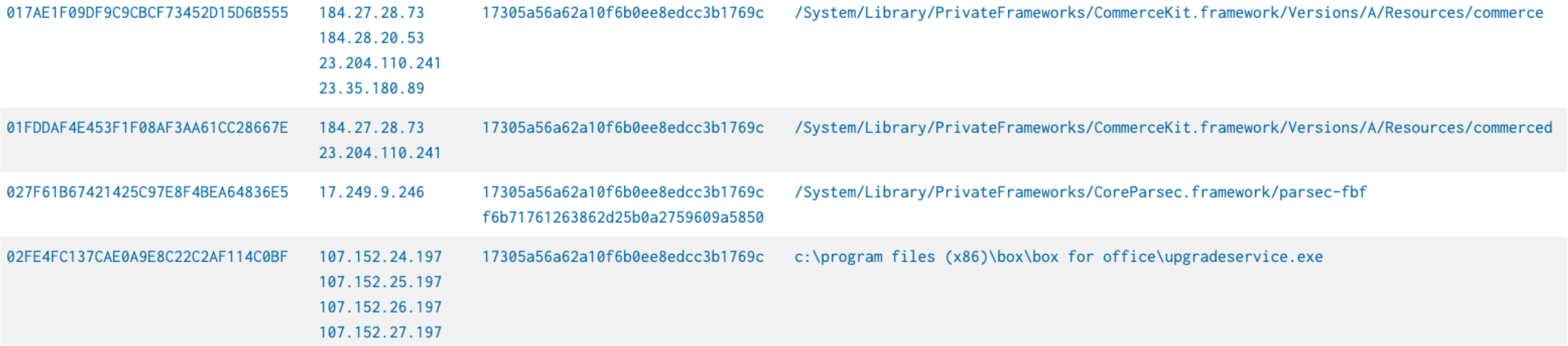


```
{ [-]
   cb_server: cbserver
   computer_name: [redacted]
   direction: outbound
   domain: fe3.delivery.mp.microsoft.com
   event_type: netconn
   local_ip: 172.[redacted]
   local_port: 56055
   md5: 8A0A29438052FAED8A2532DA50455756
   pid: 10112
   process_guid: 00003580-0000-2780-01d5-632dd3455b2f
   process_path: c:\windows\system32\svchost.exe
   protocol: 6
   proxy: false
   remote_ip: 64.4.54.18
   remote_port: 443
   sensor_id: 13696
   sha256: 7FD065BAC18C5278777AE44908101CDFED72D26FA741367F0AD4D02020787AB6
   timestamp: 1568129907.7368731
   type: ingress.event.netconn
}
```



```
{ [-]
   cb_server: cbserver
   computer_name: [redacted]
   direction: inbound
   domain:
   event_type: netconn
   local_ip: 172[redacted]
   local_port: 63773
   md5: FF9298240EC54D396520527BAF17A2C4
   pid: 188
   process_guid: 0000381d-0000-00bc-01d5-52234ce95dca
   protocol: 17
   proxy: false
   remote_ip: 208.67.222.222
   remote_port: 443
   sensor_id: 14365
   sha256: 35F889A932FD17A94B8888A85552ADC6D2A5FB769E4709CF8D681EDE6DEBC961
   timestamp: 1568048710.225299
   type: ingress.event.netconn
}
```

Round 2

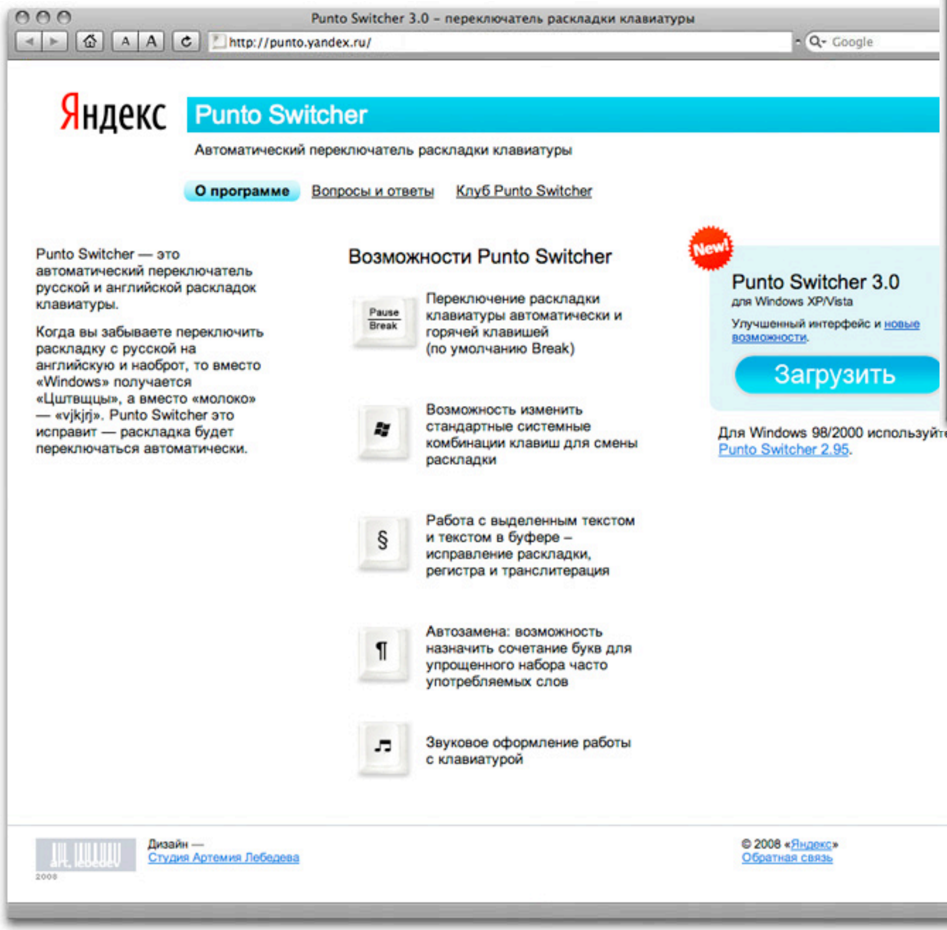


017AE1F09DF9C9CBCF73452D15D6B555	184.27.28.73 184.28.20.53 23.204.110.241 23.35.180.89	17305a56a62a10f6b0ee8edcc3b1769c	/System/Library/PrivateFrameworks/CommerceKit.framework/Versions/A/Resources/commerce
01FDDAF4E453F1F08AF3AA61CC28667E	184.27.28.73 23.204.110.241	17305a56a62a10f6b0ee8edcc3b1769c	/System/Library/PrivateFrameworks/CommerceKit.framework/Versions/A/Resources/commerced
027F61B67421425C97E8F4BEA64836E5	17.249.9.246	17305a56a62a10f6b0ee8edcc3b1769c f6b71761263862d25b0a2759609a5850	/System/Library/PrivateFrameworks/CoreParsec.framework/parsec-fbf
02FE4FC137CAE0A9E8C22C2AF114C0BF	107.152.24.197 107.152.25.197 107.152.26.197 107.152.27.197	17305a56a62a10f6b0ee8edcc3b1769c	c:\program files (x86)\box\box for office\upgradeservice.exe

```
( index=<CB Index> netconn ) OR ( index=<Zeek Index> ja3 )
| lookup ja3_dict_2.csv JA3 as ja3 output Application
| where isnull(Application)
| eval remote_ip = coalesce(id.resp_h, dest_ip, remote_ip, "null”)
| stats values(md5) as md5 values(ja3) as ja3 values(process_path) as process_path by remote_ip
| mvexpand md5
| stats values(remote_ip) as remote_ip values(ja3) as ja3 by md5
| lookup threat_intel_file_hash_lookup md5 OUTPUTNEW process_path as process_path
| search NOT(md5="") AND ja3=*
| search NOT (remote_ip=10.0.0.0/8 OR remote_ip=172.16.0.0/12 OR remote_ip=192.168.0.0/16)
```

Successes

What we found with this initial phase



Punto Switcher 3.0 – переключатель раскладки клавиатуры

http://punto.yandex.ru/

Яндекс Punto Switcher

Автоматический переключатель раскладки клавиатуры

О программе | Вопросы и ответы | Клуб Punto Switcher

Punto Switcher — это автоматический переключатель русской и английской раскладок клавиатуры.

Когда вы забываете переключить раскладку с русской на английскую и наоборот, то вместо «Windows» получается «Цштвщцы», а вместо «молоко» — «vjkjrj». Punto Switcher это исправит — раскладка будет переключаться автоматически.

Возможности Punto Switcher

- Pause Break — Переключение раскладки клавиатуры автоматически и горячей клавишей (по умолчанию Break)
- Возможность изменить стандартные системные комбинации клавиш для смены раскладки
- § — Работа с выделенным текстом и текстом в буфере – исправление раскладки, регистра и транслитерация
- ¶ — Автозамена: возможность назначить сочетание букв для упрощенного набора часто употребляемых слов
- ♫ — Звуковое оформление работы с клавиатурой

New!

Punto Switcher 3.0
для Windows XP/Vista

Улучшенный интерфейс и новые возможности.

Загрузить

Для Windows 98/2000 используйте Punto Switcher 2.95.

Дизайн — Студия Артемия Лебедева

2008

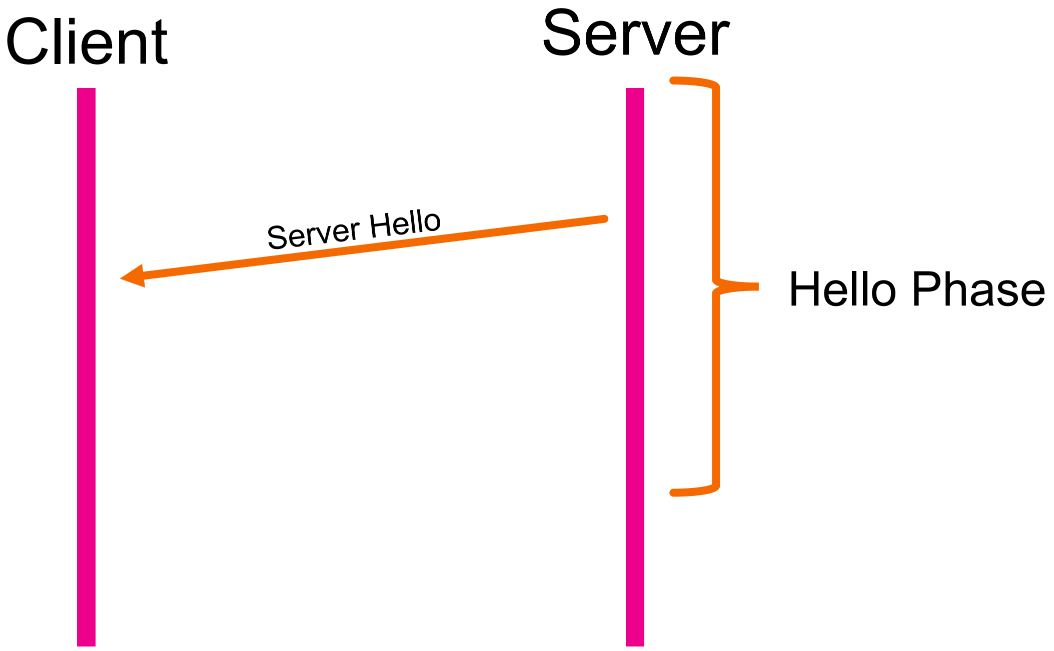
© 2008 «Яндекс»
Обратная связь

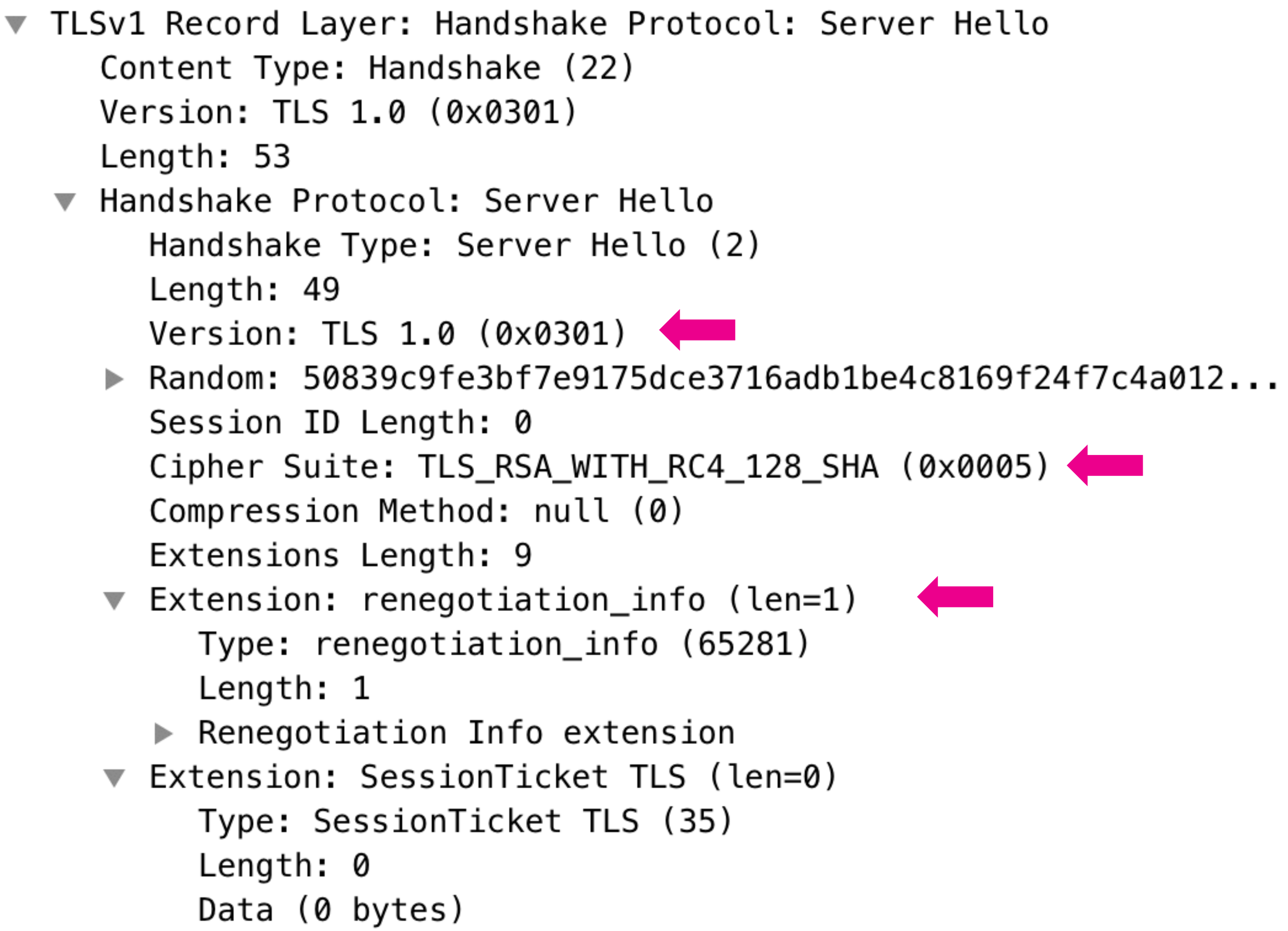
splunk> .conf19

Phase 2

JA3S

JA3S





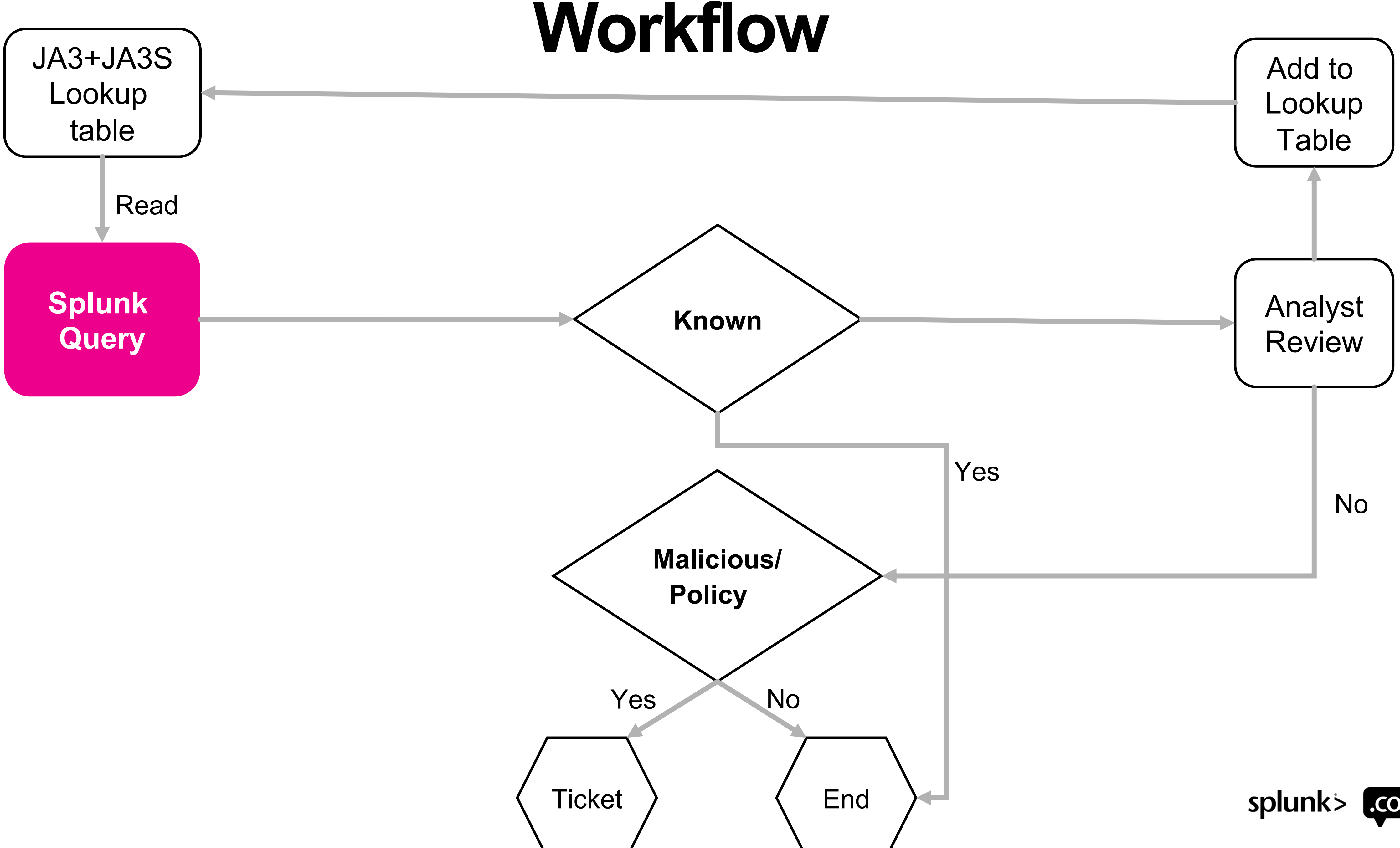
```
▼ TLSv1 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 53
  ▼ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 49
      Version: TLS 1.0 (0x0301)
    ▶ Random: 50839c9fe3bf7e9175dce3716adb1be4c8169f24f7c4a012...
      Session ID Length: 0
      Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
      Compression Method: null (0)
      Extensions Length: 9
    ▼ Extension: renegotiation_info (len=1)
        Type: renegotiation_info (65281)
        Length: 1
      ▶ Renegotiation Info extension
    ▼ Extension: SessionTicket TLS (len=0)
        Type: SessionTicket TLS (35)
        Length: 0
        Data (0 bytes)
```

769,5,65281-35

=

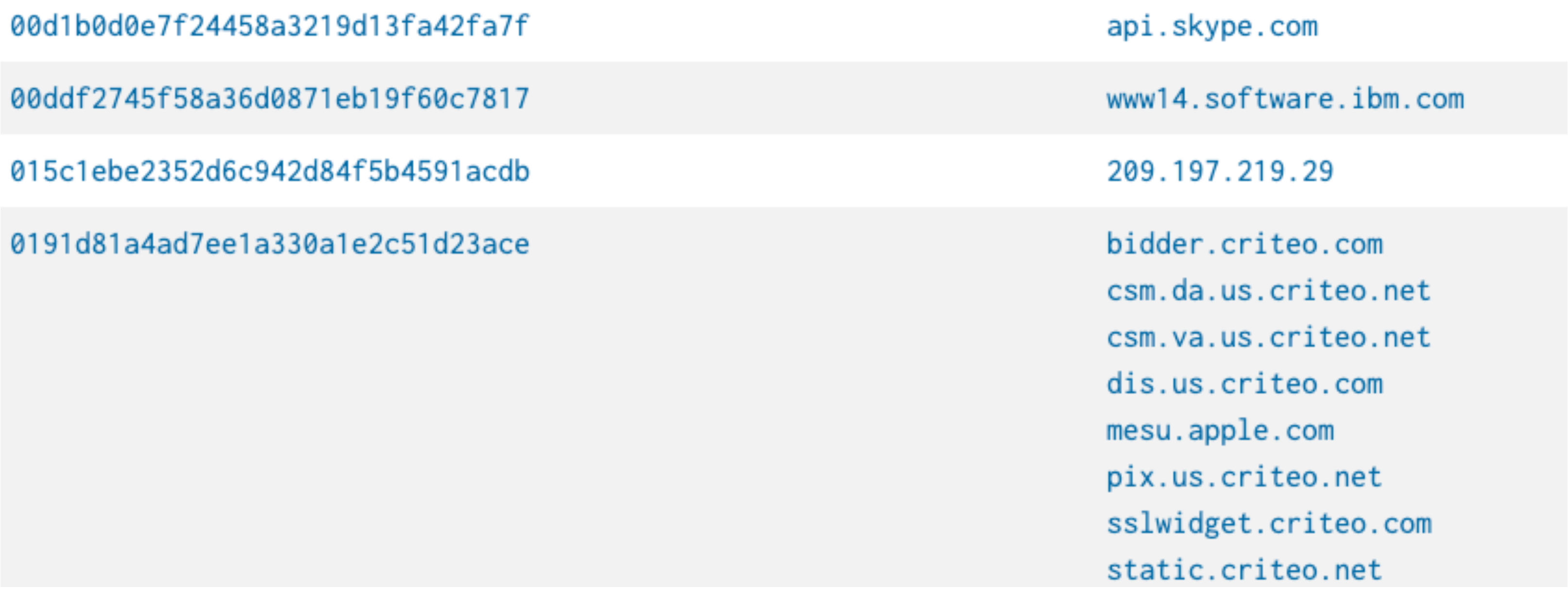
40c6454d9891ee409d90595091506207

Workflow


JA3+JA3S Lookup table
Read
Splunk Query
Known
Yes
Analyst Review
No
Add to Lookup Table
Malicious/ Policy
Yes
No
Ticket
End

JA3S

Success



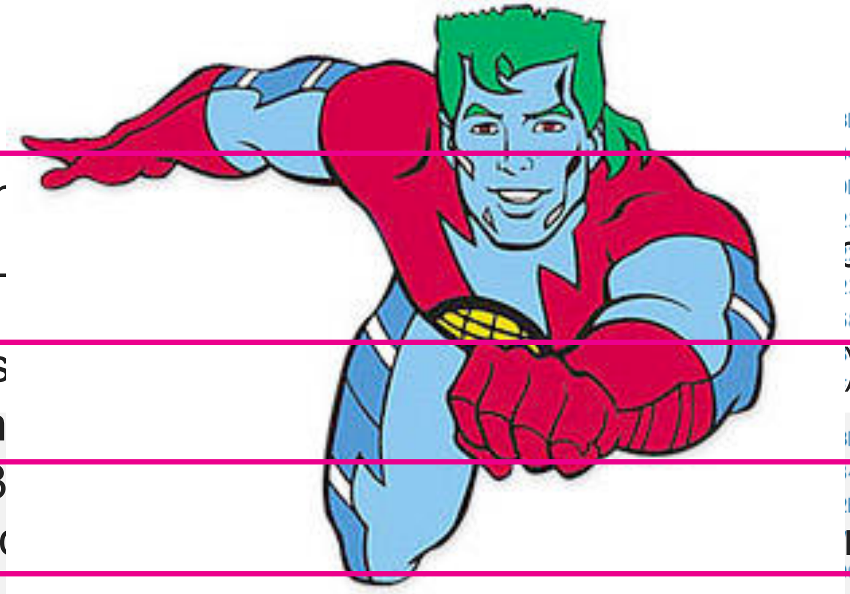
00d1b0d0e7f24458a3219d13fa42fa7f	api.skype.com
00ddf2745f58a36d0871eb19f60c7817	www14.software.ibm.com
015c1ebe2352d6c942d84f5b4591acdb	209.197.219.29
0191d81a4ad7ee1a330a1e2c51d23ace	bidder.criteo.com csm.da.us.criteo.net csm.va.us.criteo.net dis.us.criteo.com mesu.apple.com pix.us.criteo.net sslwidget.criteo.com static.criteo.net

```
index=<Zeek Index> ja3s established="true"
            NOT (dest_ip=10.0.0.0/8 OR dest_ip=172.16.0.0/12 OR dest_ip=192.168.0.0/16)
| eval dst_server = coalesce(server_name, dest_ip)
| lookup ja3s_dict.csv ja3s as ja3s output remote_server
| where isnull(remote_server)
| stats values(dst_server) as remote_server by ja3s
```

Phase 3

JA3 + JA3S

JA3+JA3S

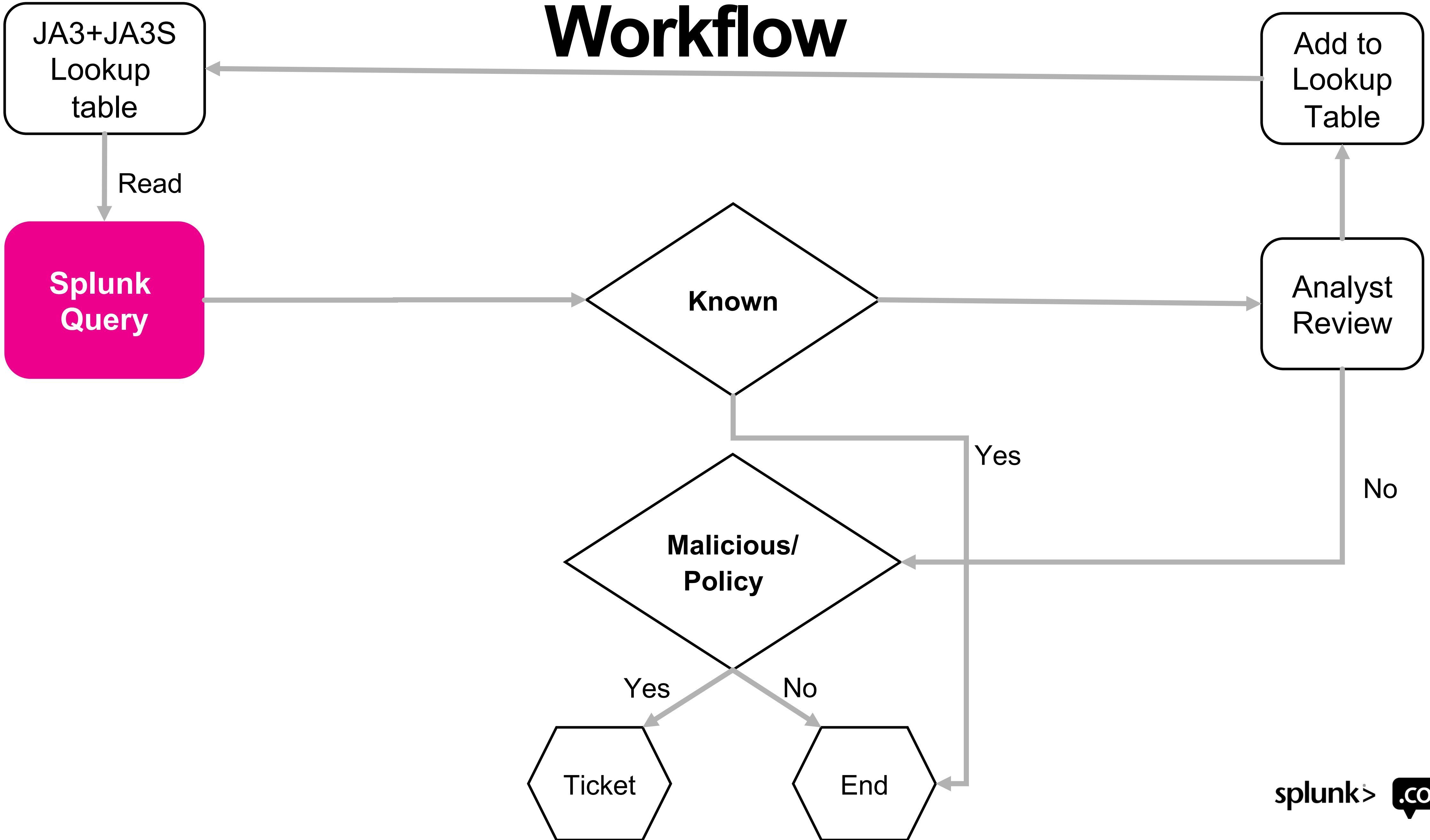


With our powers combined!

```
( index=<CB Index> netconn ) OR (ir ) | eval ja3=mvindex(ja3_lookup,0),
        NOT [| inputlookup "ja3-ja3s_
        ja3s=mvindex(ja3_lookup,1)
| eval ja3_lookup = ja3+":"+ja3s, dst_s )
| eval remote_ip = coalesce('id.resp_h
| stats values(md5) as md5 values(ja3
        values(process_path) as proc rver by remote_ip
| mvexpand md5
| stats values(remote_ip) as remote_ip values(md5) as md5 values(dst_server) as dst_server by ja3_lookup
| lookup threat_intel_file_hash_lookup md5 OUTPUTNEW process_path as process_path
| rex field=process_path "(?P<application>[^\\\^\\/]+)$"
| search NOT (md5="") AND
        ja3_lookup=* NOT (remote_ip=10.0.0.0/8 OR remote_ip=172.16.0.0/12 OR remote_ip=192.168.0.0/16)
| stats values(dst_server) as dst_server values(md5) as md5
        values(application) as application values(remote_ip) as remote_ip by ja3_lookup
```

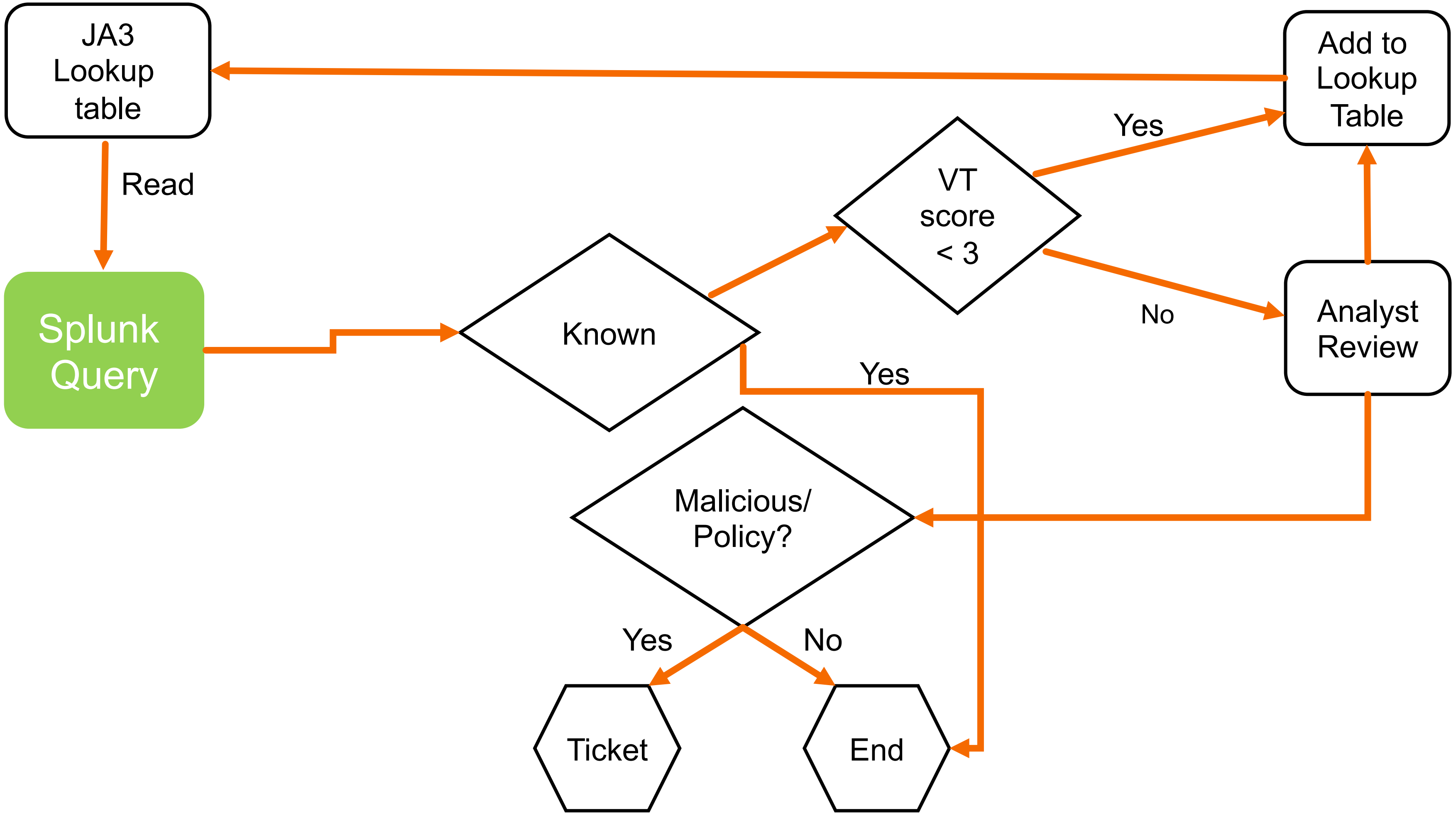
```
61b05773cda43e16a78ae1150092c068:ccc514751b175866924439bdbb5bba34      DAC36A    AssetCacheLocatorService                172.217.14.77
                                                                        4A86EE    Google Chrome Helper
                                                                        DA9765    Notes
                                                                        30AC79    Shift
                                                                        243D42    Spotify Helper
                                                                        38DCCC    chrome.exe
                                                                        89D5B1    mDNSResponder
                                                                        B2AF8
                                                                        7A2C4
61b05773cda43e16a78ae1150092c068:ea4ac9a2c0ba2e422112192cdbb985ea      DAC36A    AddressBookSourceSync                   172.217.14.106
                                                                        4A86EE    Google Chrome Helper                    172.217.5.74
                                                                        B4CBF1    Shift
                                                                                  accountsd
                                                                        C659E9    chrome.exe
                                          5CBB61D61EA8D7E588791AE56FF8BE24        com.apple.Safari.SafeBrowsing.Service
                                          6588C02C1B856998C3D41E1523AA5C0C        com.apple.WebKit.Networking
                                          698BAB9C938DB16947DAF8A6B0DA9765        firefox
                                          87C784B2FB3F8E8383C197AC0C0AF691        mDNSResponder
```

Workflow


JA3+JA3S Lookup table
Add to Lookup Table
Read
Splunk Query
Known
Analyst Review
Yes
No
Malicious/ Policy
Yes
No
Ticket
End

Operationalizing the solution

Taking the workflow and making it real



Learnings

Notes

Take-aways and Tips

JA3 lookup validation

- VT, ReversingLabs, etc…

JA3S lookup validation

- Google SafeBrowing, 3rd party reputation lists, threat intel feeds

There is LOTS of value in looking at encrypted network traffic

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION