© 2017 SPLUNK INC.

splunk> .conf2017

# Enhanced Security Monitoring

## Monitoring high risk assets/employees using behavioral baselining and correlation

Mackenzie Kyle | Attack Analysis N.A. Manager

Benji Arnold | Attack Analysis Technical Lead

September 2017 | Washington, DC

# 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.

Splunk, Splunk>, Listen to Your Data, 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. © 2017 Splunk Inc. All rights reserved.

© 2017 SPLUNK INC.

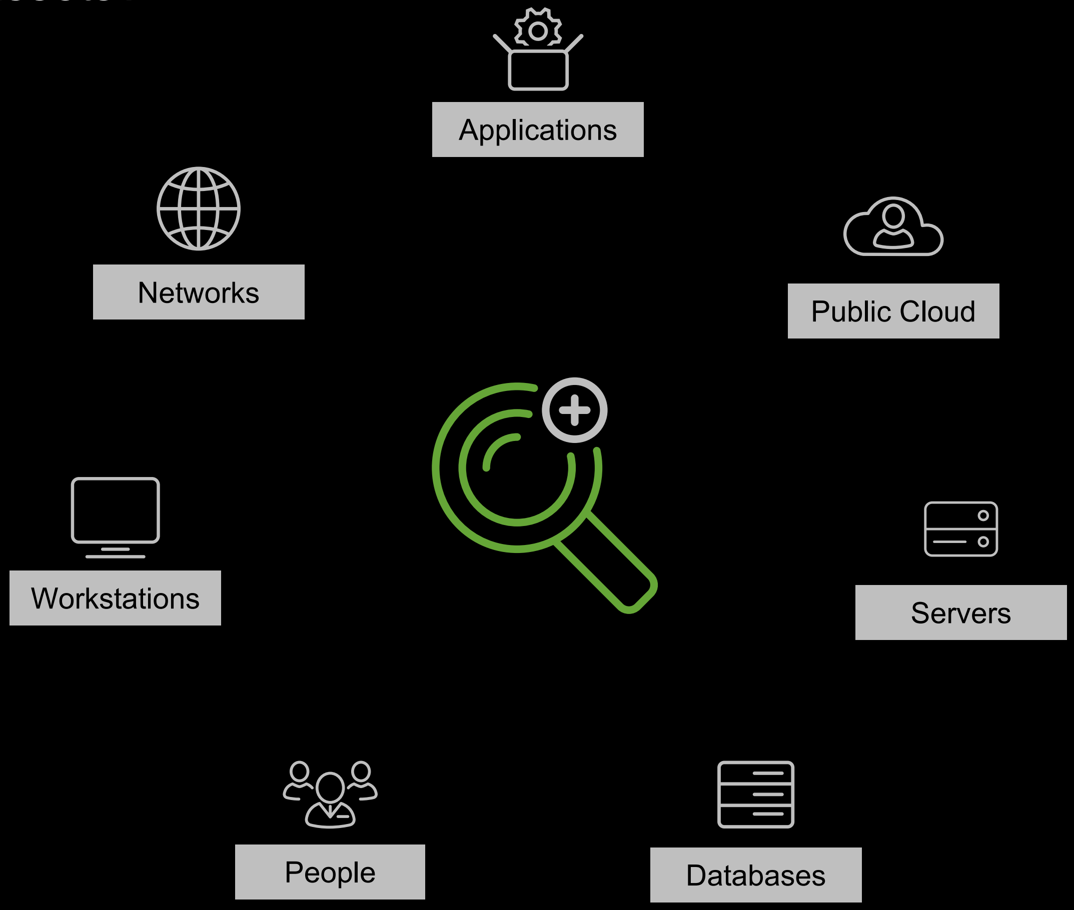
What risks have been identified for employees/assets?

What ways can we detect suspicious activity?

What type of threats are we looking for?

How do we use intelligence effectively?

What logging is available?

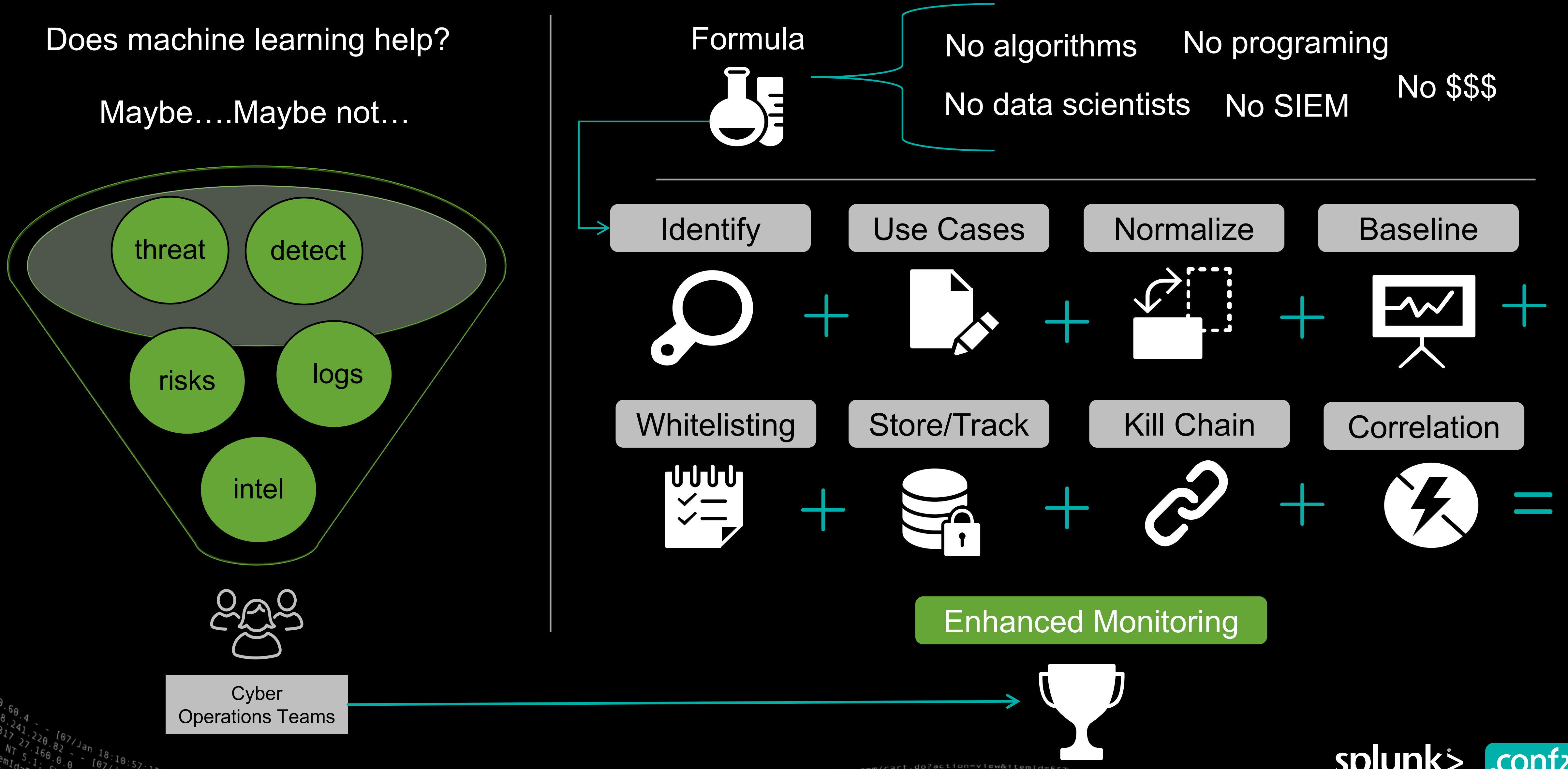


Does machine learning help?

© 2017 SPLUNK INC.

Does machine learning help?

Maybe….Maybe not…



© 2017 SPLUNK INC.

Our sample size…

2700+

## What to focus on?

What types of people, assets, or infrastructure needs to be monitored in more detail.

Think smaller groups…

Focus on criticality, classification, or high risk targets.

Use groups that are similar or relatable (ex. same roles, types of assets).

Publicized FI Events

## Use Threat Intelligence

Use publically available information to determine who or what is at high risk of targeting?

Think about what adversaries are after...

Do any employees have publically facing roles?

Have there been recent attacks targeting infrastructure or business processes that you maintain?

Multiple Lines of Business

## Business Input

Use feedback from the business to gather your requirements.

Think about protecting long term or future business processes.

Do they have audit or regulatory requirements?

Insider threats or can you leverage to support time sensitive investigations?

© 2017 SPLUNK INC.

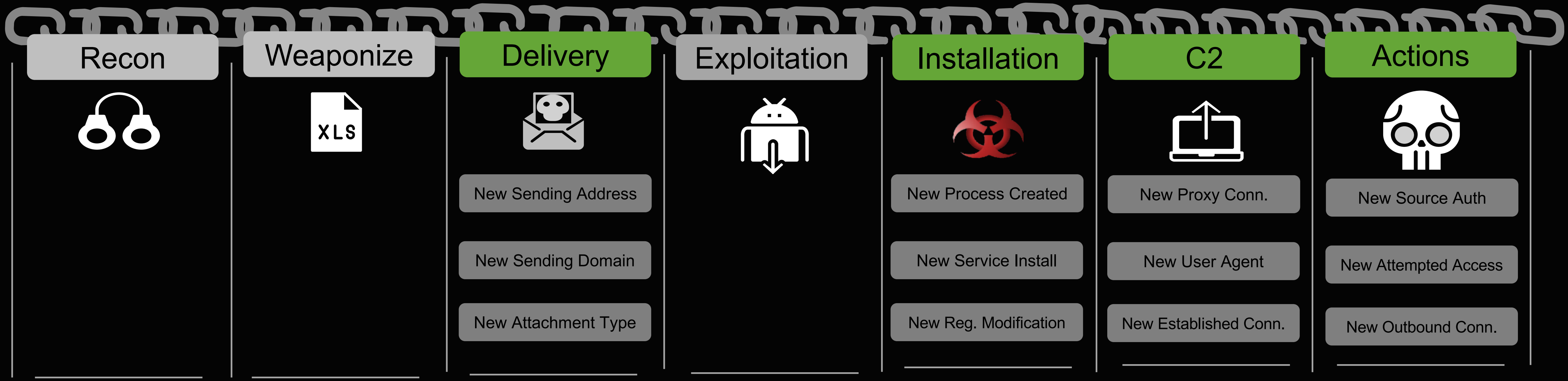
## Defining Your Use Cases

Using a methodology like the Kill Chain makes it easier to organize your stages of possible detection.

The use cases should apply to only data sets that can track new activity. There are no signature based detection use cases here.

Try to develop use cases that can detect in the earlier stages.

Use cases may change subject to the monitoring group (ex. applications vs employees).



| Recon | Weaponize | Delivery | Exploitation | Installation | C2 | Actions |
|---|---|---|---|---|---|---|
|  |  | New Sending Address |  | New Process Created | New Proxy Conn. | New Source Auth |
|  |  | New Sending Domain |  | New Service Install | New User Agent | New Attempted Access |
|  |  | New Attachment Type |  | New Reg. Modification | New Established Conn. | New Outbound Conn. |

© 2017 SPLUNK INC.

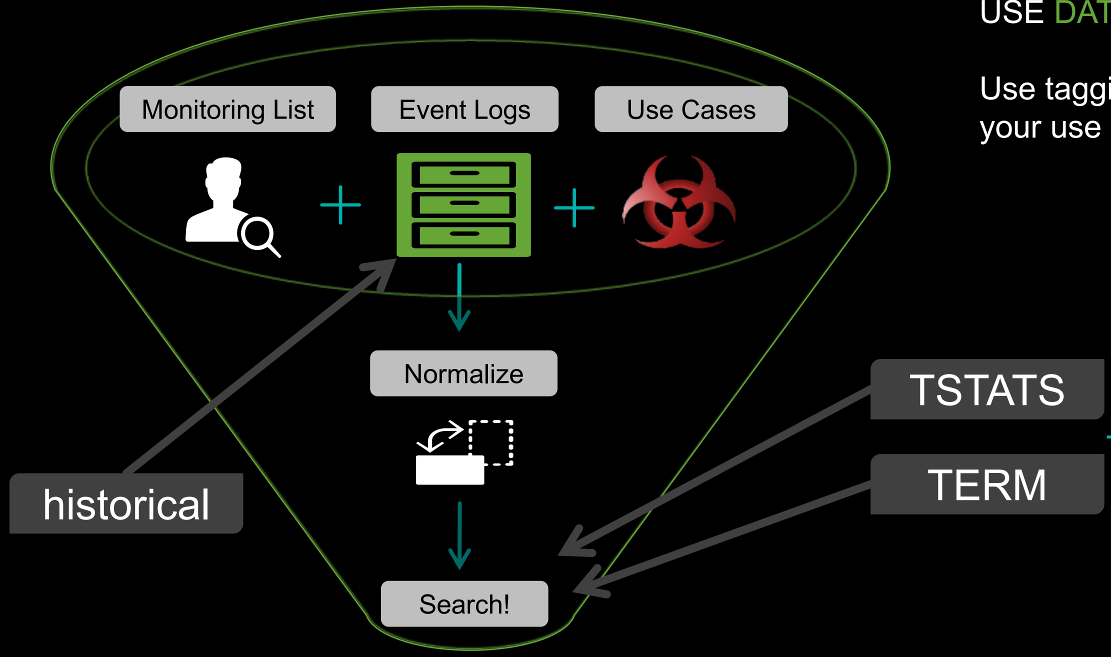
# Developing Your Baseline

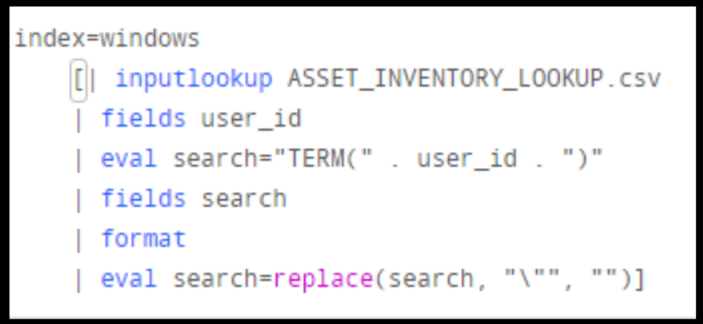
Ensure you have at least 90 days worth of data for your baseline – the more the better!

Do not start baselining until you have built a data dictionary – use Common Information Model.

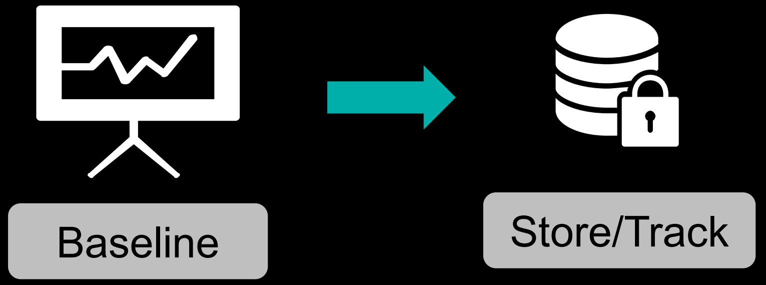
USE DATA MODELS WHEN POSSIBLE!

Use tagging, event types, and source types to organize your summary index. Try and clearly label your use cases within the index.





```
index=windows
    [| inputlookup ASSET_INVENTORY_LOOKUP.csv
    | fields user_id
    | eval search="TERM(" . user_id . ")"
    | fields search
    | format
    | eval search=replace(search, "\"", "")]
```

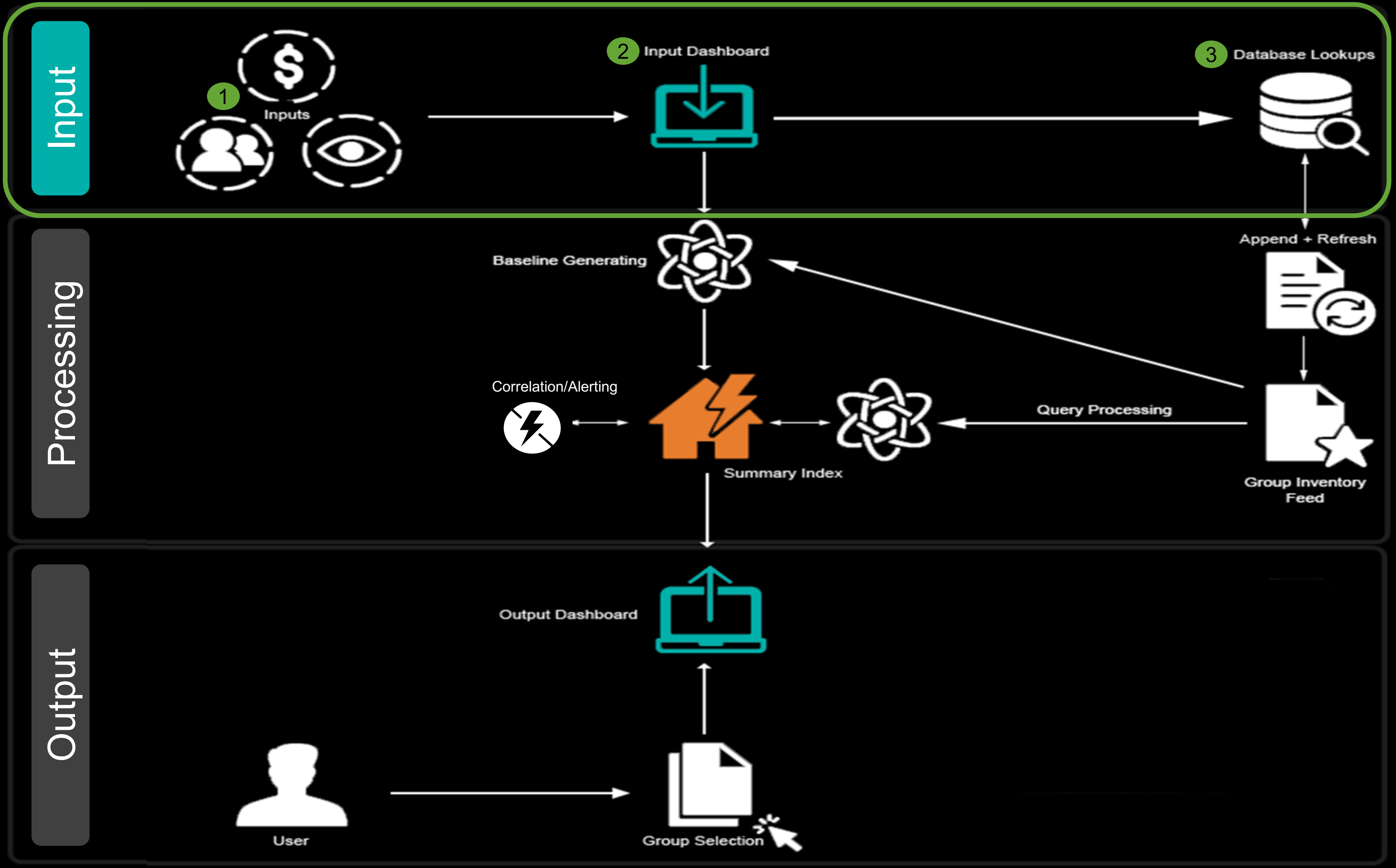


Your summary index will be your master whitelist that tracks all new events per day.

It will be used for all new event tracking and correlation!

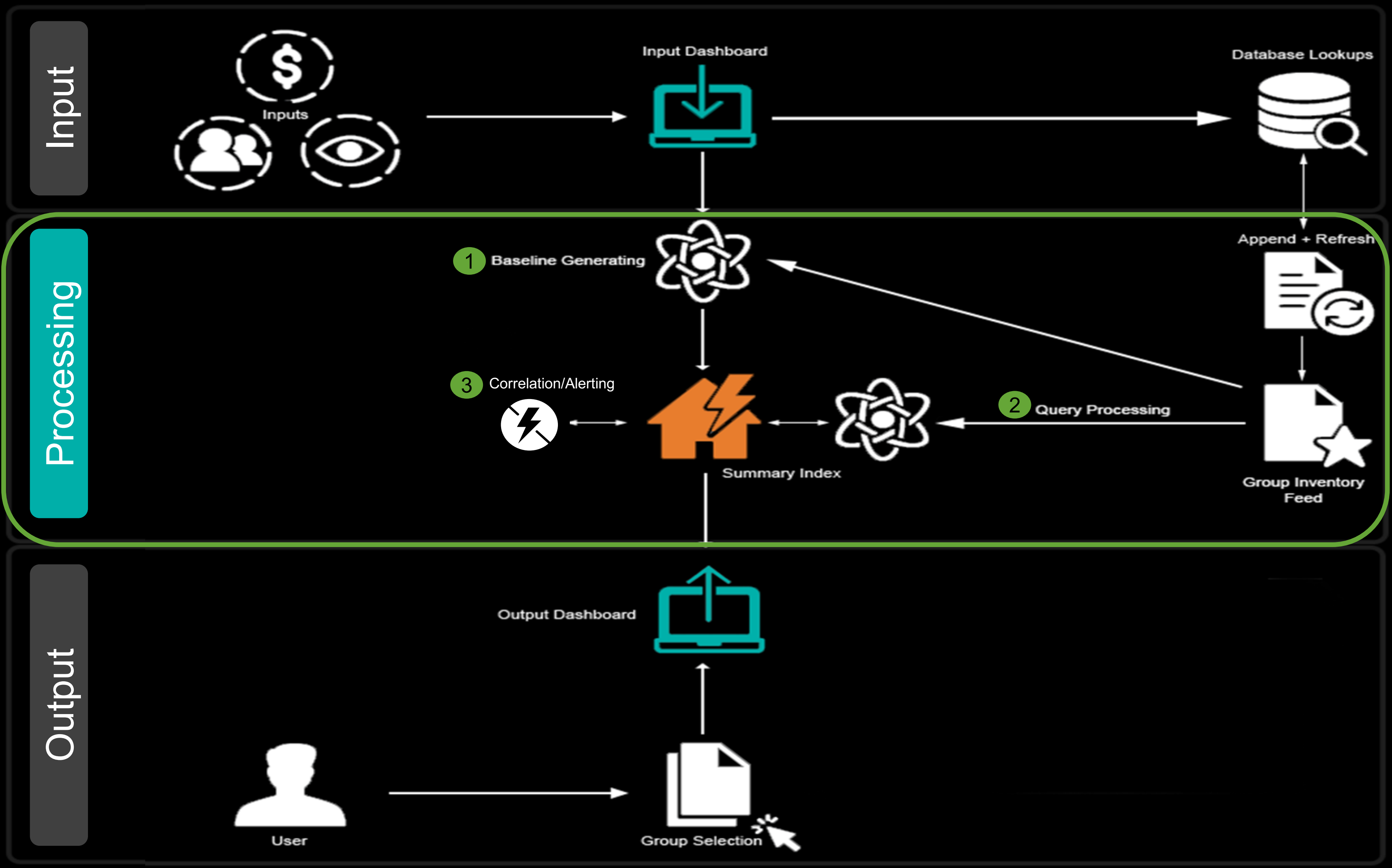
splunk> .conf2017

© 2017 SPLUNK INC.



1. **Employee Inputs**
   - User ID
   - Asset Name
   - Risk/Access Levels
   - Group ID
2. **Input Dashboard**
   - Submit IDs to Monitor
   - Employees, Assets, Apps
3. **Database Lookups**
   - Asset/Employee Inventory Systems
   - Store Dynamic List – Update Often

© 2017 SPLUNK INC.



## 1 Baseline Generating

- Baseline Activity by Group ID
- Baseline Per Use Case – TAG!
- Output Events to summary index
- Keep Index for >1 Year, Update Daily

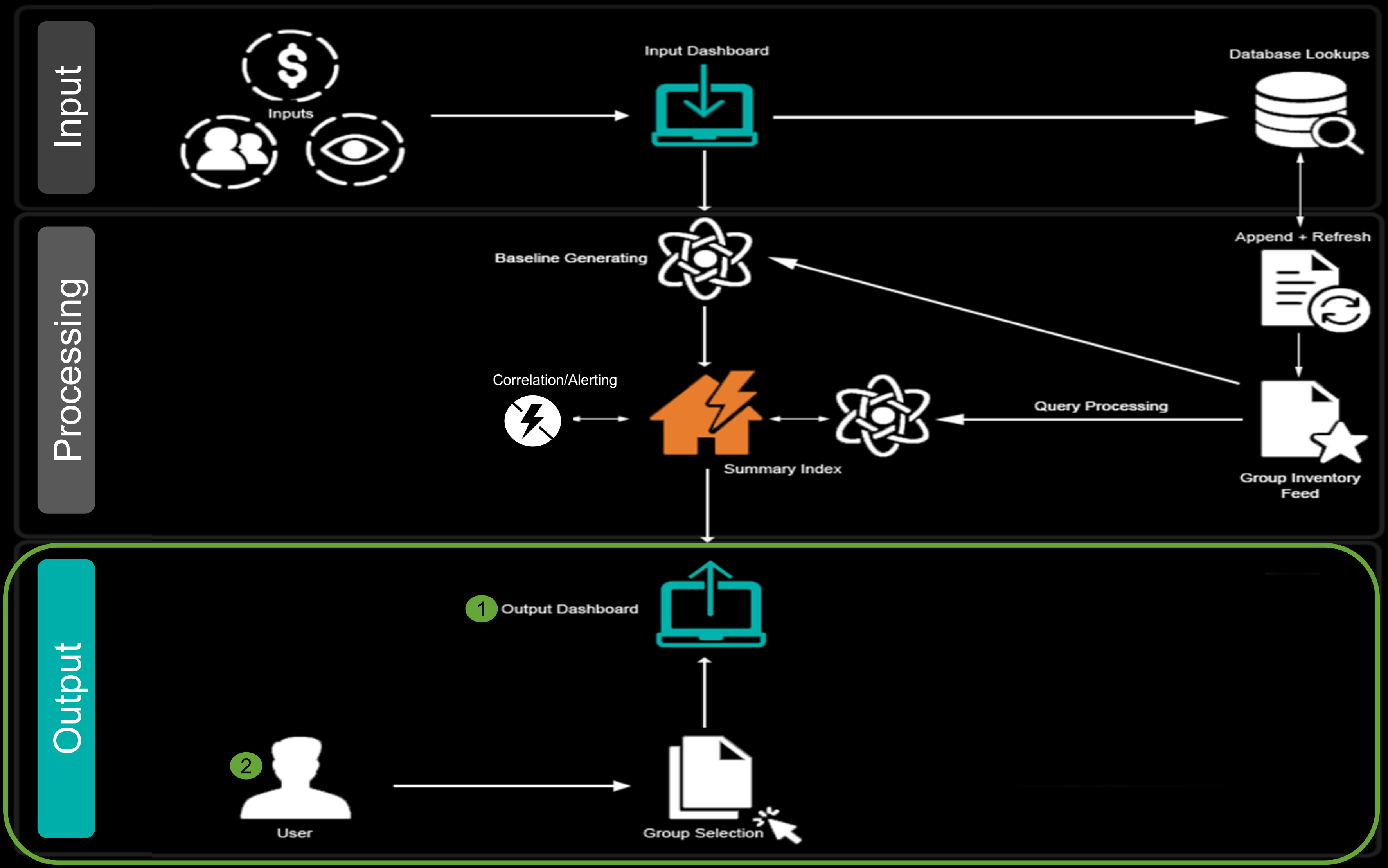
## 2 Query Processing

- Use input list to find events per use case
- Use summary index to detect "new" event
- Only continue to track/store new events per day
- Run scheduled queries at least once a day

## 3 Correlation/Alerting

- Build correlation using the kill chain
- Machine Learning toolkit on top of summary index

© 2017 SPLUNK INC.



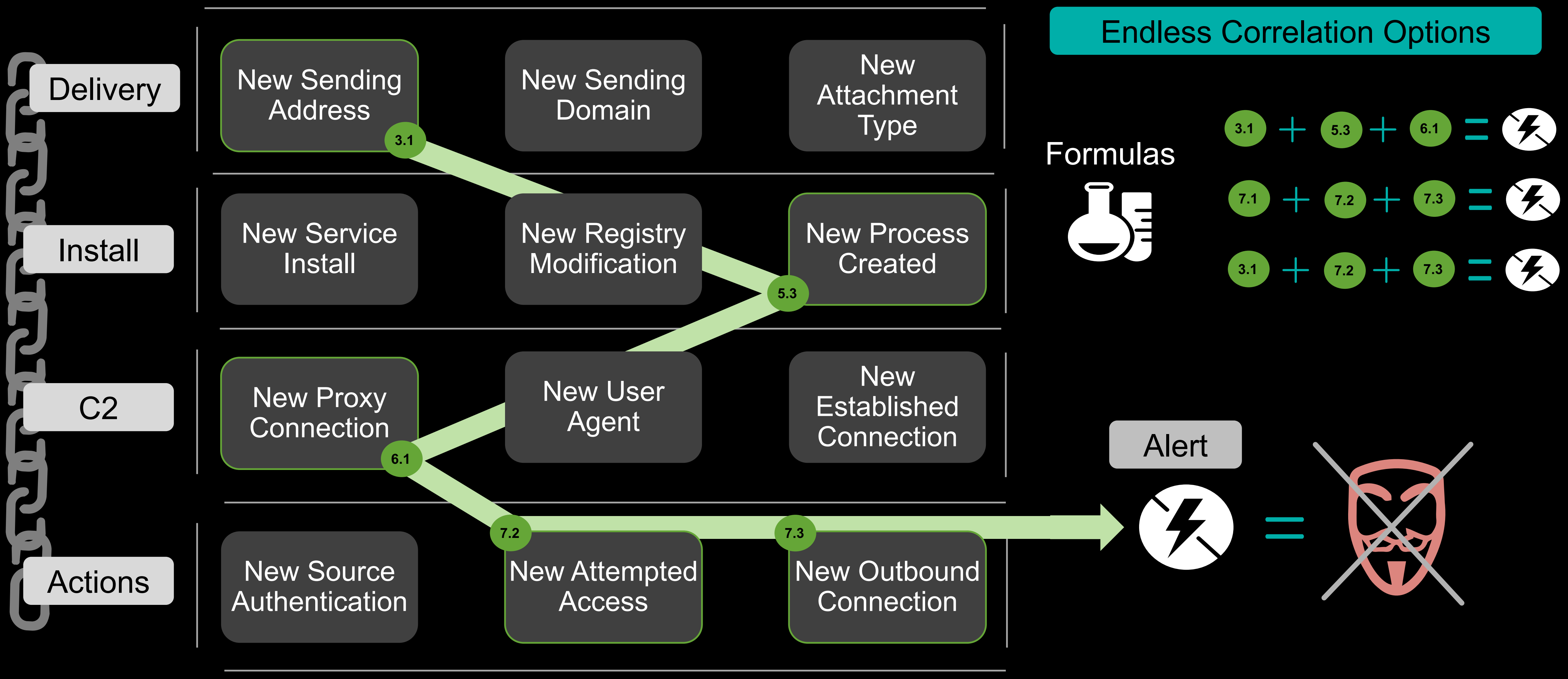
1 **Output Dashboard**

- Used to visualize the results
- Show critical use cases only
- Interactive – multiple teams can access
- Can leverage with other analytics methods

2 **Analysis/Hunting**

- Data can be used for multiple purposes
- Easier to find threats with organized data

© 2017 SPLUNK INC.



| | | | |
|---|---|---|---|
| Delivery | New Sending Address (3.1) | New Sending Domain | New Attachment Type |
| Install | New Service Install | New Registry Modification | New Process Created (5.3) |
| C2 | New Proxy Connection (6.1) | New User Agent | New Established Connection |
| Actions | New Source Authentication | New Attempted Access (7.2) | New Outbound Connection (7.3) |

## Endless Correlation Options

Formulas

3.1 + 5.3 + 6.1 = ⚡

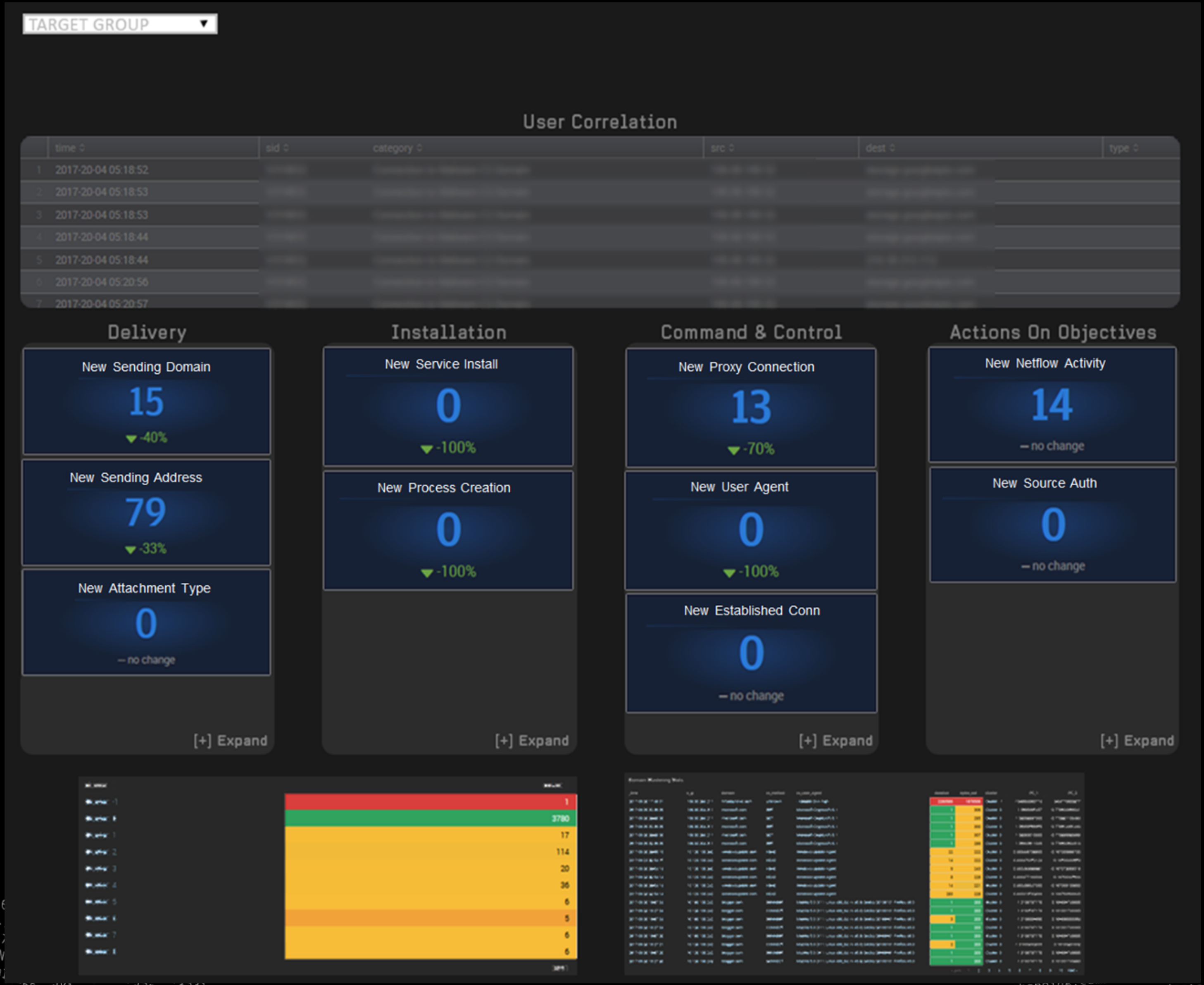
7.1 + 7.2 + 7.3 = ⚡

3.1 + 7.2 + 7.3 = ⚡

Alert

⚡ =

© 2017 SPLUNK INC.



## User Correlation

|  | time | sid | category | src | dest | type |
|---|---|---|---|---|---|---|
| 1 | 2017-20-04 05:18:52 | [redacted] | [redacted] | [redacted] | [redacted] |  |
| 2 | 2017-20-04 05:18:53 | [redacted] | [redacted] | [redacted] | [redacted] |  |
| 3 | 2017-20-04 05:18:53 | [redacted] | [redacted] | [redacted] | [redacted] |  |
| 4 | 2017-20-04 05:18:44 | [redacted] | [redacted] | [redacted] | [redacted] |  |
| 5 | 2017-20-04 05:18:44 | [redacted] | [redacted] | [redacted] | [redacted] |  |
| 6 | 2017-20-04 05:20:56 | [redacted] | [redacted] | [redacted] | [redacted] |  |
| 7 | 2017-20-04 05:20:57 | [redacted] | [redacted] | [redacted] | [redacted] |  |

### Delivery

New Sending Domain
15
▼ -40%

New Sending Address
79
▼ -33%

New Attachment Type
0
– no change

[+] Expand

### Installation

New Service Install
0
▼ -100%

New Process Creation
0
▼ -100%

[+] Expand

### Command & Control

New Proxy Connection
13
▼ -70%

New User Agent
0
▼ -100%

New Established Conn
0
– no change

[+] Expand

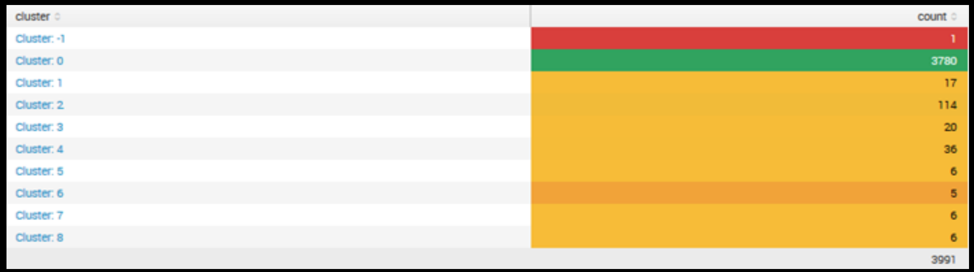
### Actions On Objectives

New Netflow Activity
14
– no change

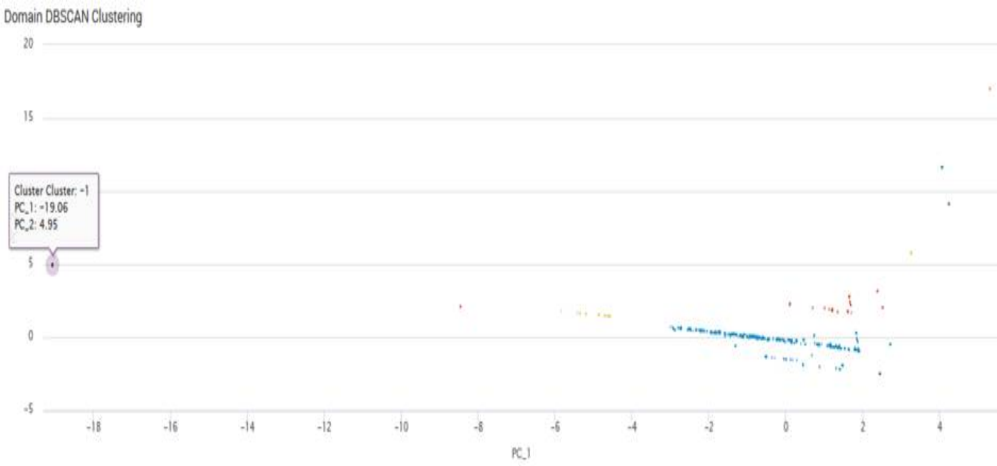
New Source Auth
0
– no change

[+] Expand

## Machine Learning Toolkit



| cluster | count |
|---|---|
| Cluster: -1 | 1 |
| Cluster: 0 | 3780 |
| Cluster: 1 | 17 |
| Cluster: 2 | 114 |
| Cluster: 3 | 20 |
| Cluster: 4 | 36 |
| Cluster: 5 | 6 |
| Cluster: 6 | 5 |
| Cluster: 7 | 6 |
| Cluster: 8 | 6 |
|  | 3991 |



© 2017 SPLUNK INC.

## Pros

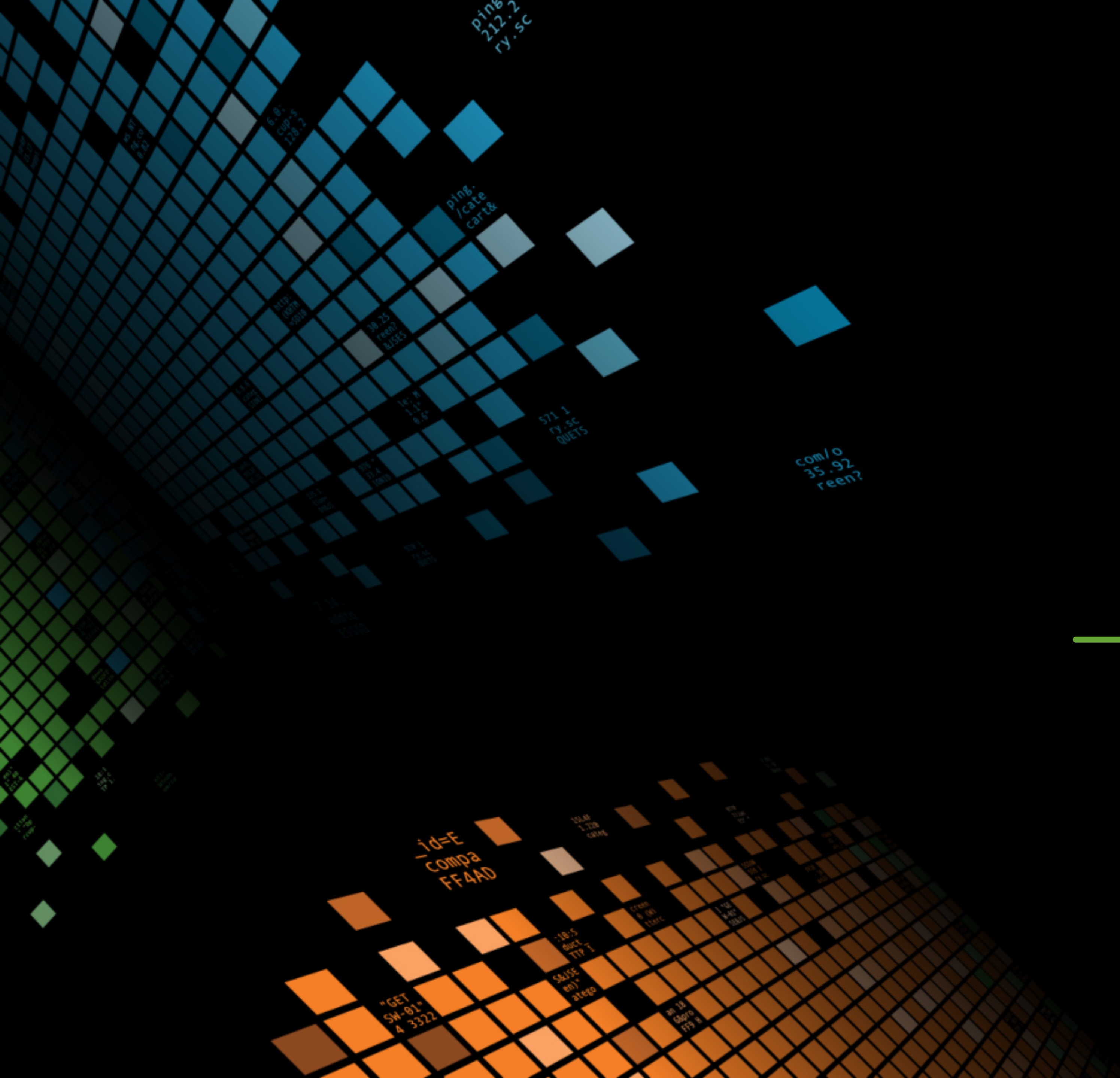
1. Splunk Enterprise Only! Does not require any additional $$$!
2. You don’t need to be a data scientist, cyber expert, or machine learning guru to create and deploy.
3. You are able to monitor small to moderate sized groups fairly quickly.
4. You can be flexible with the use case development and correlation. You can create multiple alerts across events in >1 kill chain stages, or just within 1 stage.
5. The summary index will track all new events per use case each day, and can be indexed for as long as you’d like. You can always use the historical index for hunting and not just for alerting.
6. You can create the monitoring dashboard using HTML with your own custom JavaScript, CSS, etc. This makes it easier for other groups outside Ops to use if needed (Employee Investigations, Threat Intel, etc.).
7. The method is flexible, you can use to monitor for suspicious activity on targeting employees, application servers, etc.
8. Maintenance is minimal, once the use cases are developed there is not much overhead to maintain.
9. You may catch a targeted threat!

## Cons

1. It takes a long time to normalize and build out your data dictionary. If you do not have an effective feed onboarding strategy it will require a lot of effort.
2. This is not intended for large groups of assets, the idea is to monitor smaller groups of assets or employees. Larger groups will require additional software or storage and can be hard to scale.
3. New events don’t always indicate malicious activity, if your previous baselining whitelist contained adversarial activity, you likely will ignore it using this method.

Questions?

© 2017 SPLUNK INC.



# Q&A

© 2017 SPLUNK INC.

# Thank You

Don't forget to **rate this session** in the .conf2017 mobile app

splunk> .conf2017