

Step Up Your Defenses with End-to-End Detection, Investigation, and Response

Bhavin Patel & Jose Hernandez
Security Researchers | Splunk

Forward-Looking Statements



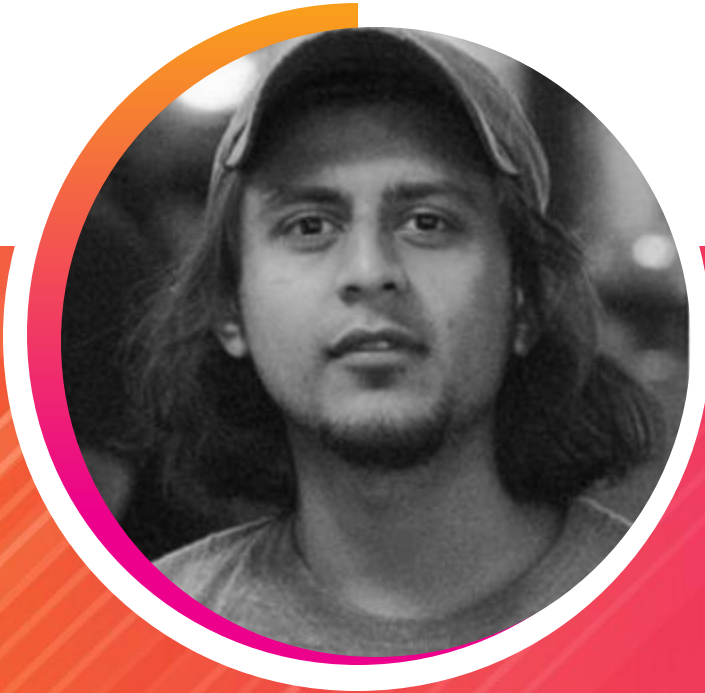
During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. 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.

Step Up Your Defenses with End-to-End Detection, Investigation, and Response

© 2019 SPLUNK INC.



Bhavin Patel

- Incident Response @NBCUniversal
- Security Research Team @Splunk
- Bass Player @TheFamilyFlaw
- Slackliner in making



Jose Hernandez

- Former Prolexic/Akamai Architect
- Co-founded Zenedge, which was acquired by Oracle
- Long time Splunker, recently returned to do research



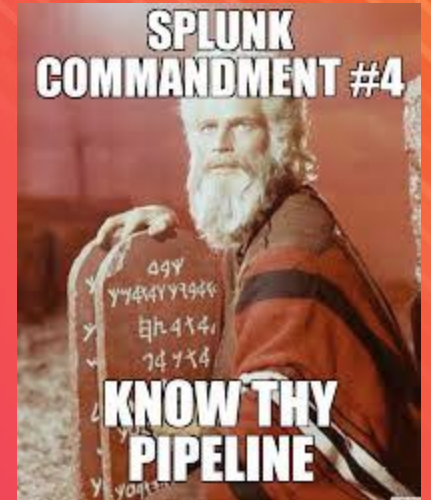
Agenda

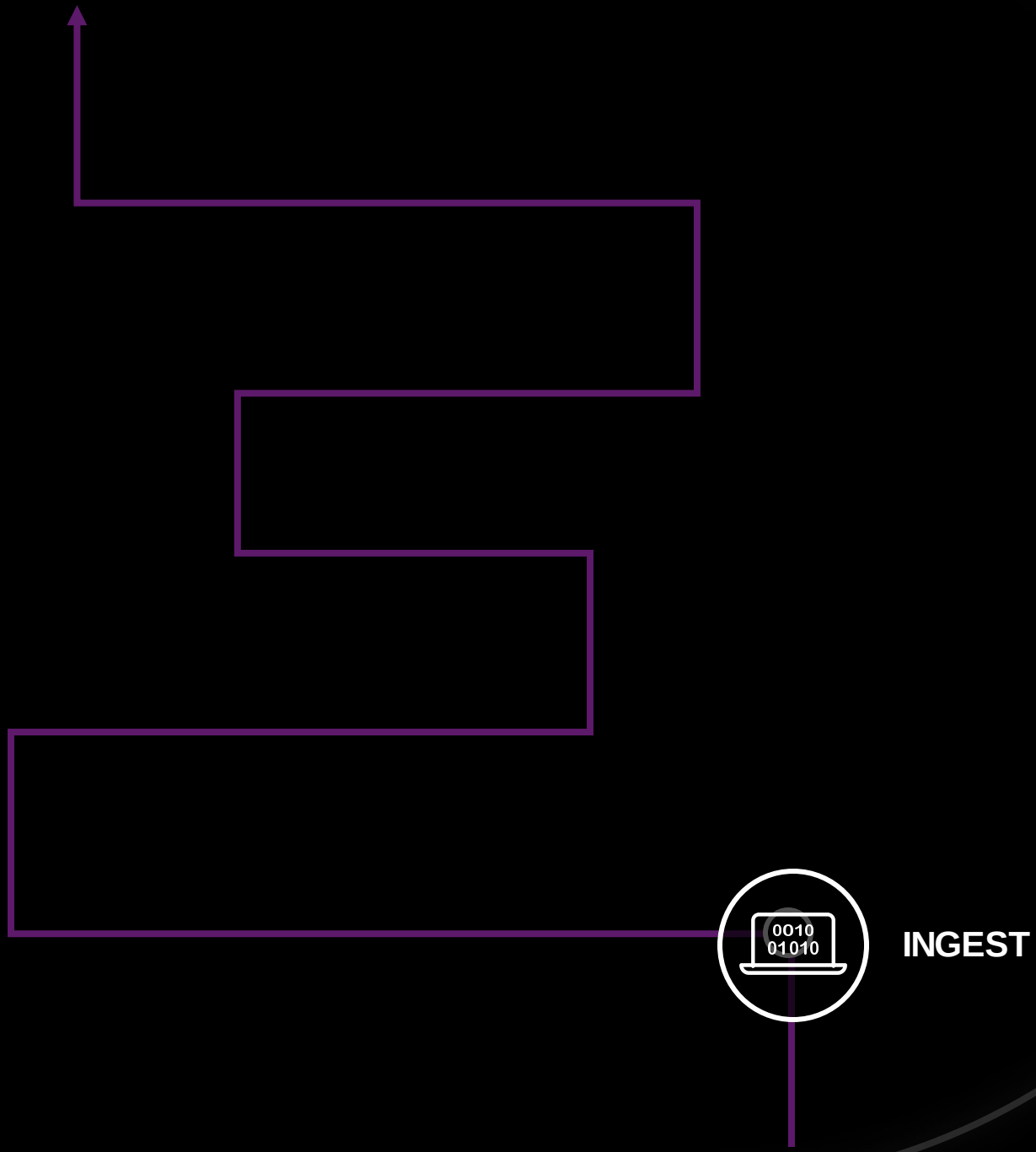
- Data Journey
- Splunk Security Portfolio & Splunk Content Offerings
- How is SecOps doing?
- ESCU v1.0 lessons learned
- Content Evolution
- Next Steps
- Demo
- Takeaways and Q&A



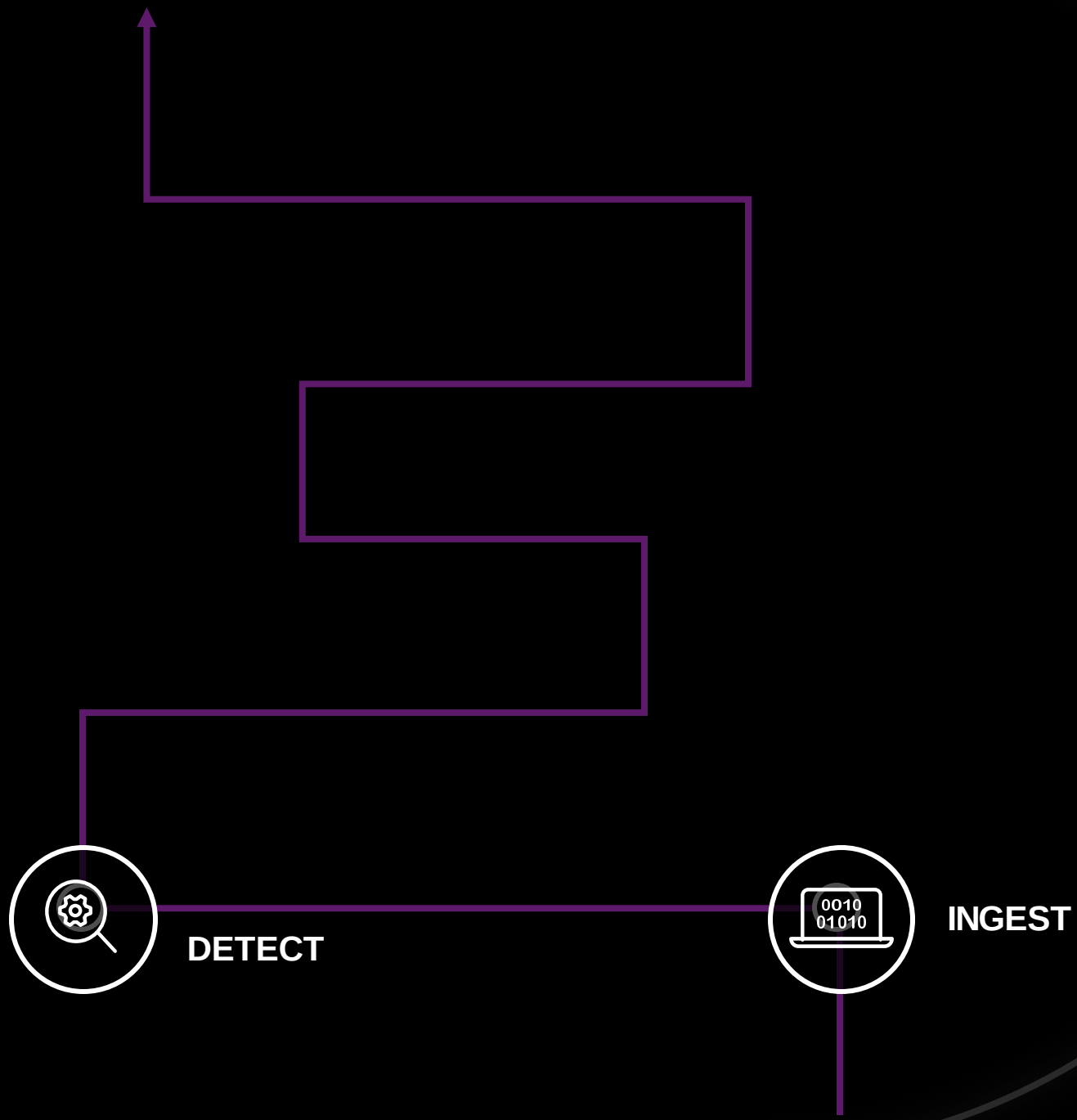
Data Journey

Overview

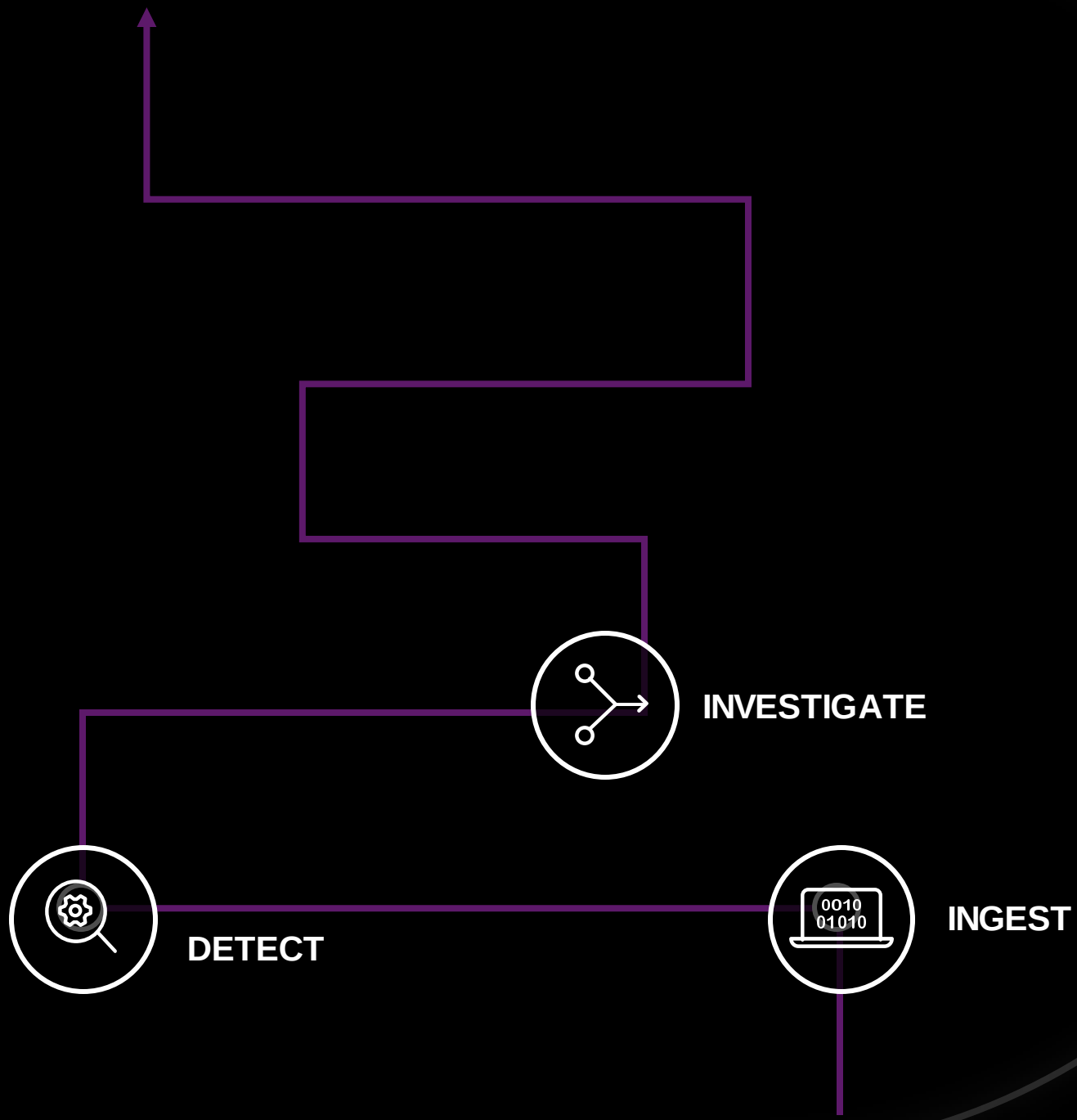




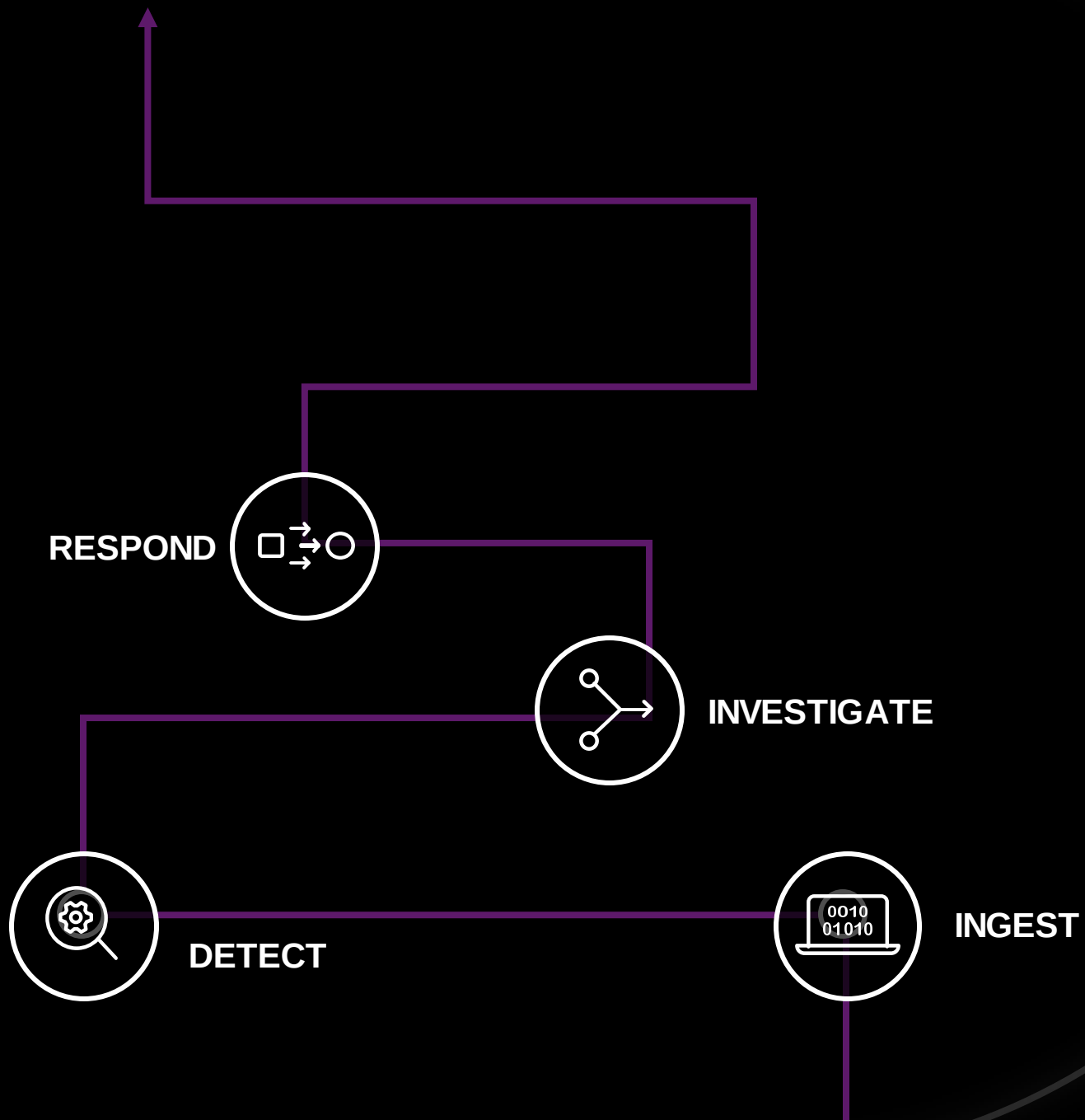
Our view of typical data journey



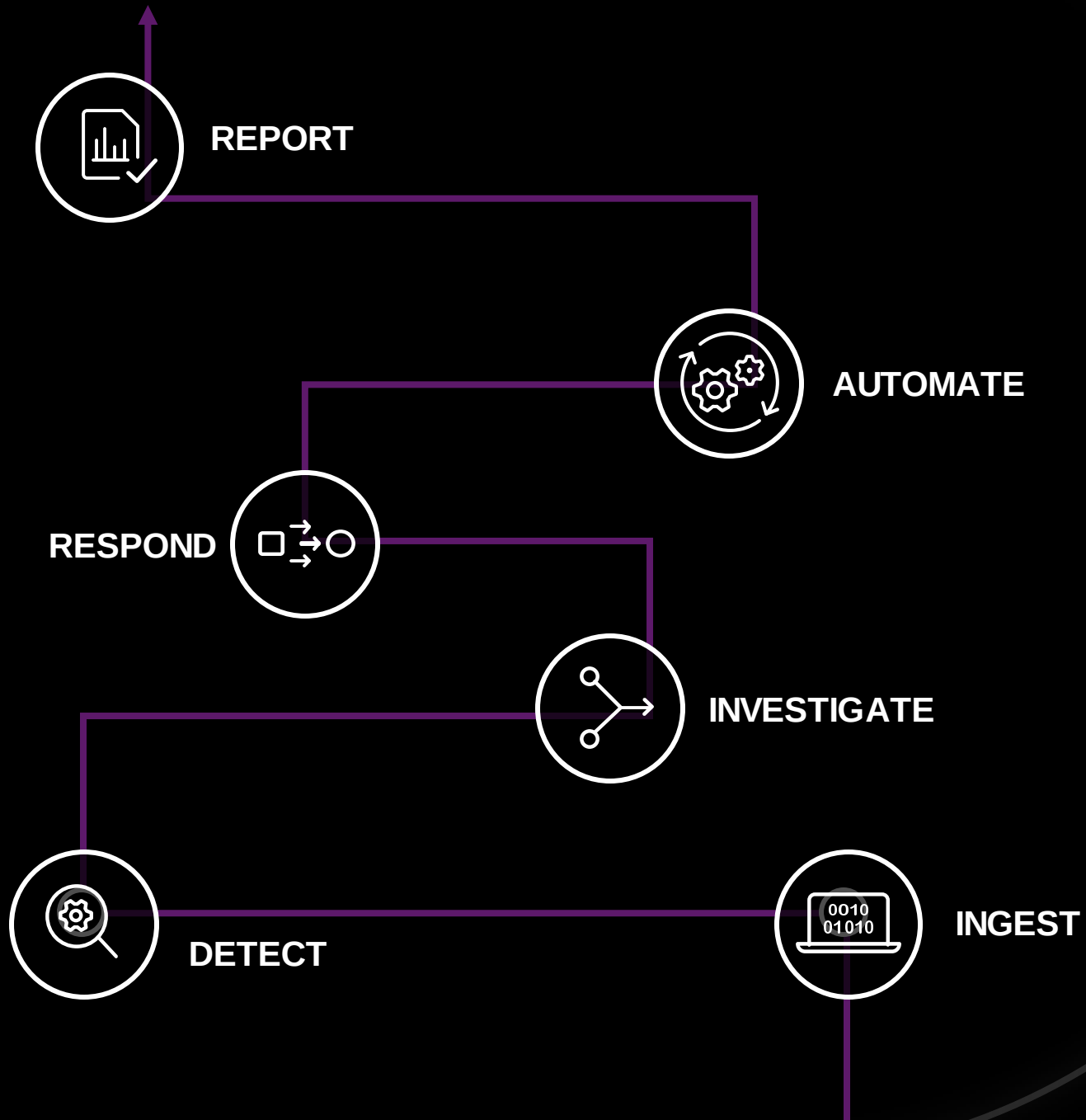
Our view of typical data journey



Our view of typical data journey



Our view of typical data journey



Our view of typical data journey

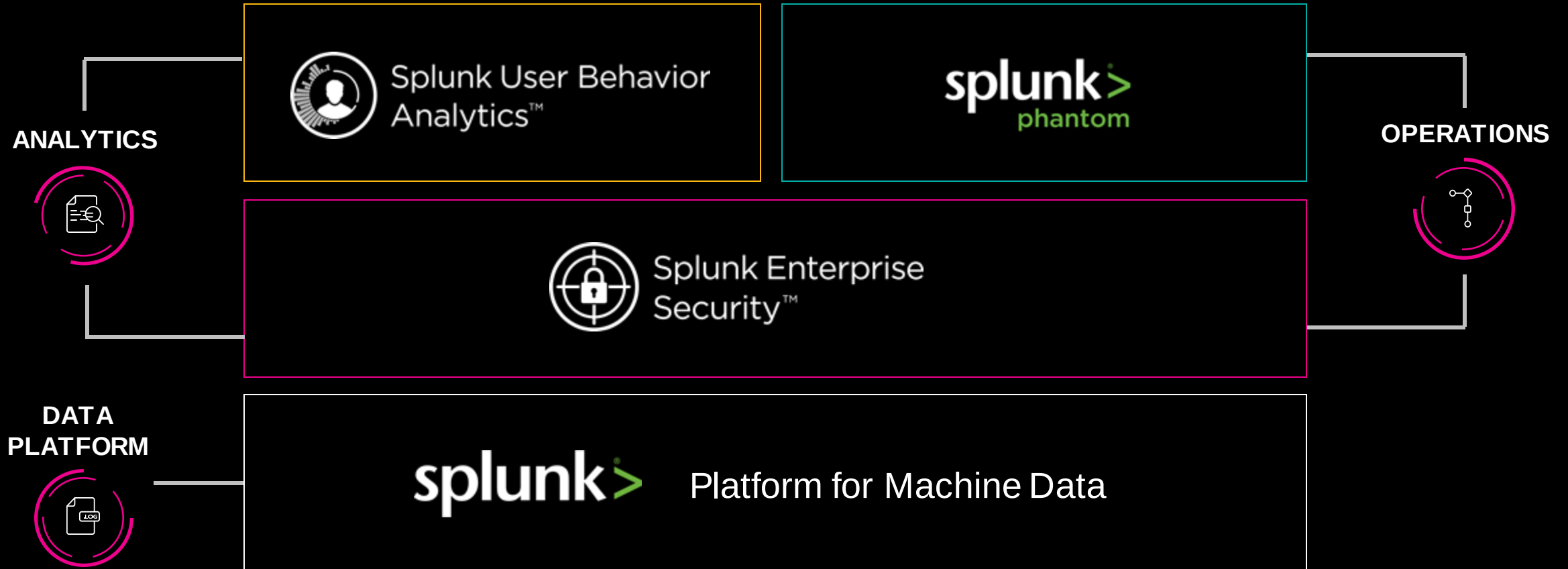


Splunk Security Portfolio

Overview

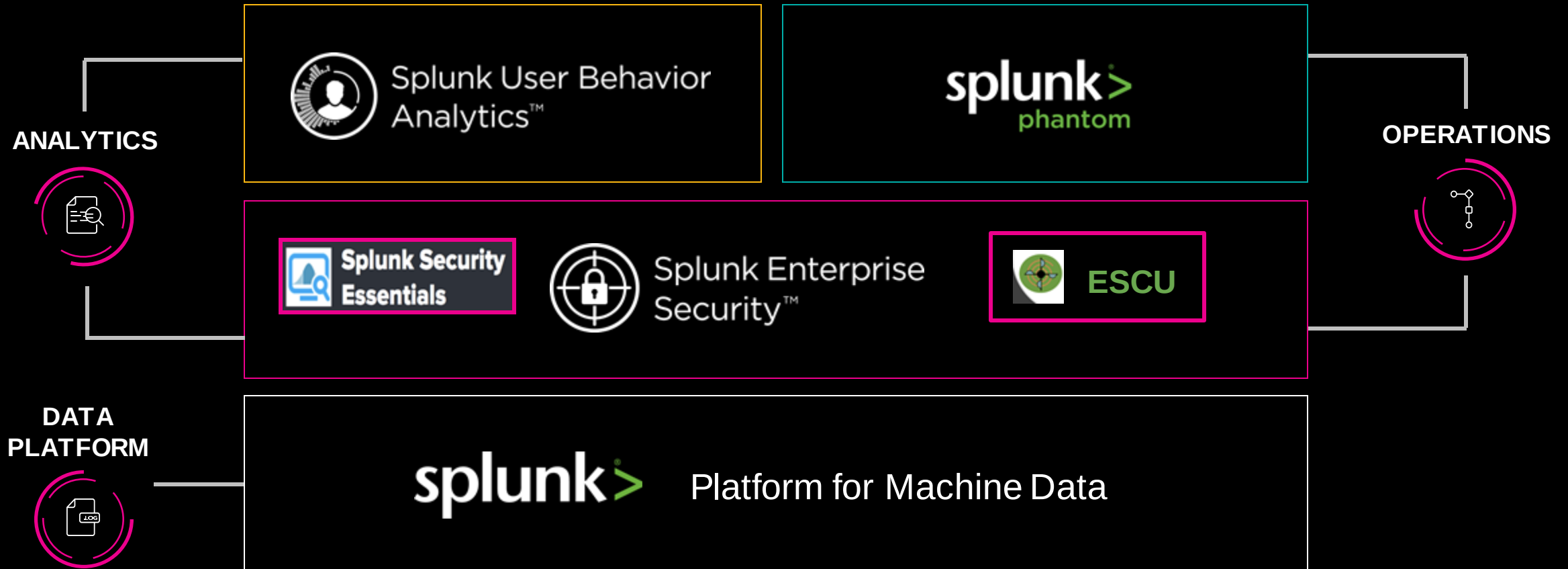


Splunk Security Portfolio



```
010100101010101010101101010110101010101011010101101010101010110101001010010
10101010101101010110101010101011010101101101010101011010100101001010101010
10110101011010101010101101010110110101010101101010111010110100100100001010
011
```

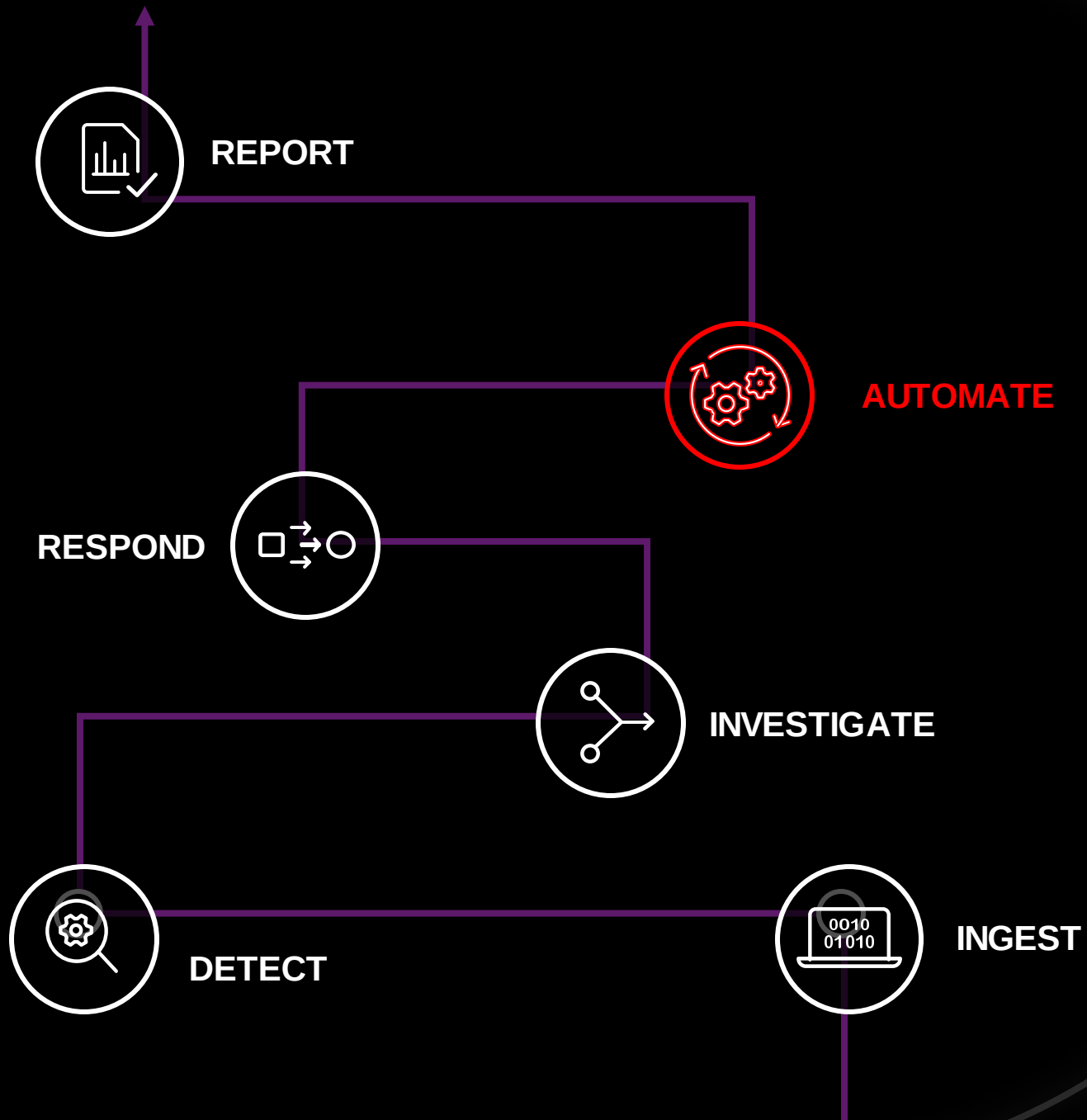
Splunk Security Portfolio



01010010101010101010110101010101010101011010101101010101010101001010010
10101010101101010110101010101011010101101101010101011010100101001010101010
10110101011010101010101101010110110101010101101010111010110100100100001010
011

Current State of Security Operations







Splunk Content Offerings

.....it's all over the place



Enterprise Security

© 2019 SPLUNK INC.



Content Offered

- **Correlation** Searches
- **Event sequencing** templates
- **Adaptive response** actions
- **Frameworks**
 - Notable
 - Risk Analysis
 - Threat Intelligence

Value-Add

- **Pre-built searches** to detect known risky or malicious activity by correlating one or multiple sources
- Produce **risk events** for low confident alerts and notables for high confident alerts
- **Event sequencing** to correlate multiple risk events or notables based on a sequence or risk
- Adaptive response actions to run pre-configured actions across Splunk and other integrated tools

Phantom

© 2019 SPLUNK INC.



Content Offered

- **Apps**
- **Playbooks**
- Case templates

Value-Add

- Purpose built **playbooks** to help investigate and respond to a detection that can be used OOTB or customized to organizational requirements
- **Automate** repeated investigative/response actions/workflows for SOC efficiency
- Leverage Phantom apps to connect to existing security solutions in your environment and perform **actions through APIs**

UBA



Content Offered

- **Anomaly Models**
 - Detection
 - Contextual
 - IOC
- **Threat Models**
 - Specialized threat detection
 - Graph/kill-chain analysis
- **Threat Rules**

Value-Add

- Multi-pass **machine learning models** to detect threats based on IOCs, anomalies, static/dynamic contextual information to reduce false-positives
- Correlation of **behavioral** and **signature** based alerts for broader context
- **Identity Resolution**
- Known & Unknown threat detection



Enterprise Security Content Updates

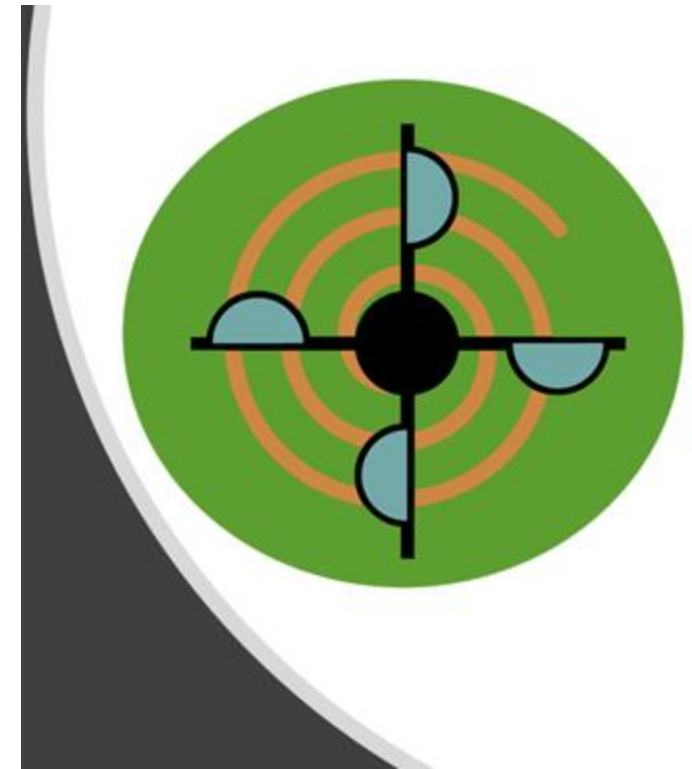
Version 1.0



Enterprise Security Content Updates

Version 1.0

- ESCU delivers security analysis guides called **Analytic Stories** packaged in a Splunk application.
- An analytic story v1.0 is composed of:
 - **Detection** searches
 - **Support** searches
 - **Investigative** searches
 - **Contextual** searches
- 60+ Analytic Stories , 200+ Detections and Investigations
- Maps to MITRE ATT&CK, Cyber Kill Chain, NIST, CIS



Enterprise Security

Use Case Library

Analytic Story Details: DNS Hijacking

Use Case: Adversary Tactics
[Back to Use Case Library](#)

Created: _____ N/A
 Last Modified: _____ 2019-03-21
 Version: _____ 1

Description
 Secure your environment against DNS hijacks with searches that help you detect and investigate unauthorized changes to DNS records.

Narrative
 Dubbed the Achilles heel of the Internet (see <https://www.ft.com/labs/articles/threat-intelligence/dns-is-still-the-achilles-heel-of-the-internet-25613>), DNS plays a critical role in routing web traffic but is notoriously vulnerable to attack. One reason is its distributed nature. It relies on unstructured connections between millions of clients and servers over inherently insecure protocols. The gravity and extent of the importance of securing DNS from attacks is undeniable. The fallout of compromised DNS can be disastrous. Not only can hackers bring down an entire business, they can intercept confidential information, emails, and login credentials, as well.

On January 22, 2019, the US Department of Homeland Security 2019's Cybersecurity and Infrastructure Security Agency (CISA) raised awareness of some of the risks of attacks against infrastructure, both in the United States and abroad. It issued Emergency Directive 19-01 (see <https://cyberdhs.gov/ed/19-01/>), which summarizes the actions agencies to take the following four actions, all within 10 days:

1. For all .gov or other agency-managed domains, audit public DNS records on all authoritative and secondary DNS servers, verify that they are accurate, and report any discrepancies to CISA.
2. Update the passwords for all accounts on systems that can make changes to each agency's 2019's DNS records.
3. Implement multi-factor authentication (MFA) for all accounts on systems that can make changes to each agency's 2019 DNS records or, if impossible, provide CISA with the names of systems, the reasons why MFA cannot be enabled within the required timeline, and an ETA for when it can be enabled.
4. CISA will begin regular delivery of newly added certificates to Certificate Transparency (CT) logs for agency domains via the Cyber Hygiene service. Upon receipt, agencies must immediately begin monitoring CT log data for certificates issued that they did not request. If an agency confirms that a certificate was unauthorized, it must report the certificate to the issuing certificate authority and to CISA. Of course, it makes sense to put equivalent actions in place within your environment, as well.

In DNS hijacking, the attacker assumes control over an account or makes use of a DNS service exploit to make changes to DNS records. Once they gain access, attackers can substitute their own MX records, name-server records, and addresses, redirecting emails and traffic through their infrastructure, where they can read, copy, or modify information seen. They can also generate valid encryption certificates to help them avoid browser-certificate checks. In one notable attack on the Internet service provider, GoDaddy, the hackers altered Sender Policy Framework (SPF) records a relatively minor change that did not inflict excessive damage but allowed for more effective spam campaigns.

The searches in this Analytic Story can help you detect and investigate DNS hijacking that may indicate that DNS hijacking has taken place within your environment.

References

- <https://www.ft.com/labs/articles/threat-intelligence/dns-is-still-the-achilles-heel-of-the-internet-25613>
- <https://www.ft.com/labs/articles/threat-intelligence/dns-is-still-the-achilles-heel-of-the-internet-25613>
- <https://www.ft.com/labs/articles/threat-intelligence/dns-is-still-the-achilles-heel-of-the-internet-25613>
- <https://www.ft.com/labs/articles/threat-intelligence/dns-is-still-the-achilles-heel-of-the-internet-25613>
- <https://www.ft.com/labs/articles/threat-intelligence/dns-is-still-the-achilles-heel-of-the-internet-25613>

Framework mappings

CIS 20

KILL CHAIN PHASES

ATTACK

NIST

TECHNOLOGIES

content across Detect, Investigate & Response

Explanation, how to implement, known FPs for a detection

Data source dependency

ESCU - DNS record changed - Rule

Description
 The search takes the DNS records and their present results of the discovered_dns_records status and finds if any records have changed by searching DNS response from the Network_BasicIndex dataset across the last day.

Explanation

Search

How to implement

Known False Positives

Cyber Security Framework Attributes

CIS 20

KILL CHAIN PHASES

ATTACK

NIST

Data Sources (Technology)

What Was Missing in ESCU v1.0?

We could not integrate **UBA** and **Phantom** into our security analytics

It did not have the ability to have **tightly coupled** detection objects with baseline, investigation and response objects

It lacked the fields needed to **automate** an analytic story end to end



Enterprise Security Content Updates

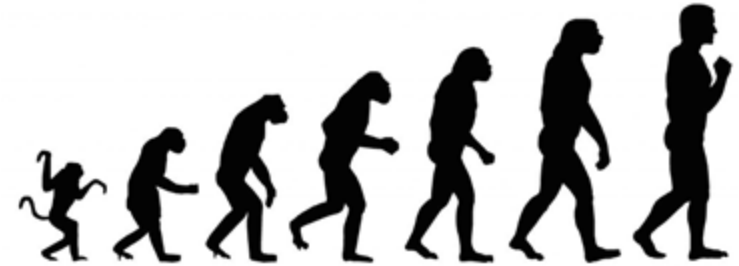
Version 2.0



What's Evolved?

ESCU support **multiple** products at all phases of our workflow

- UBA detections
- Phantom detections
- Phantom investigations
- UBA investigations
- Phantom responses



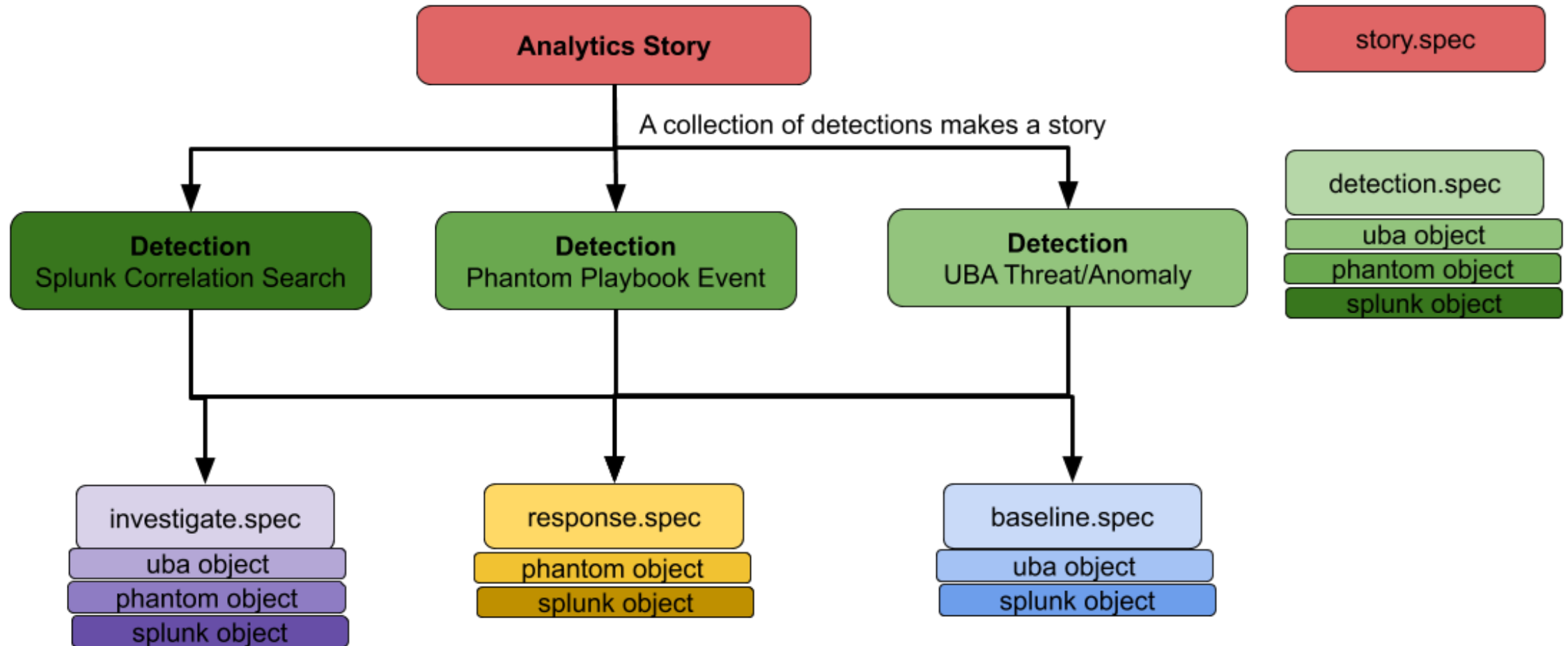
A structure that can expand with **new product introductions**

An ability link **entities** necessary to “**run a story end to end**”

Allow **metadata** mapping for all pieces of content

Introduced **new tagging** like updated ATT&CK, updated categories to match Splunk Security Essentials, and Security Use case.

Analytic Story Design



Each detection has a set of Investigations
Responses and Base lines

Content Specification 2.0

New Specs <https://github.com/splunk/security-content/tree/develop/spec/v2>

- baselines.spec.json
- detections.spec.json
- investigations.spec.json
- responses.spec.json
- story.spec.json

New tools under <https://github.com/splunk/security-content/tree/develop/bin>

- Validate.py
- Generate.py

Analytic Story

```
"usecase": "Advanced Threat Detection",  
"detections": [  
  {  
    "detection_id": "1169w17b-ef78-4b59-aae8-5369073014e1",  
    "name": "DNS record changed",  
    "type": "splunk"  
  },  
  {  
    "detection_id": "8129w27b-ef78-4w59-aae8-5369073014e1",  
    "name": "Lateral Movement detected",  
    "type": "uba"  
  },  
  {  
    "detection_id": "1229w27b-ef78-4w59-aae8-5369073014e1",  
    "name": "Playbook that detects DNS Hijacks",  
    "type": "phantom"  
  }  
],
```

Detection Object

Each detection object will have:

- associated baseline objects
- detection object
- associated investigation objects
- associated response objects

```
{
  "baselines": [
    {
      "id": "2296f721-8842-42ce-bfc7-74bd8c72b7c3",
      "name": "Discover DNS records",
      "product_type": "splunk"
    }
  ],
  "detect": {
    "splunk": {
      "correlation_rule": {
        "notable": {
          "risk": {
            "scheduling": {
              "suppress": {
                "search": ""
              }
            }
          }
        }
      }
    }
  },
  "entities": ["dest"]
  "investigations": [
    {
      "id": "e211a8cf-35e7-4bb2-8140-e756cc06fd72",
      "name": "Get DNS Server History for a host",
      "product_type": "splunk"
    },
    {
      "id": "c096f721-8842-42ce-bfc7-74bd8c72b711",
      "name": "DNS record change investigation",
      "product_type": "phantom"
    }
  ]
}
```

Behind the Scenes

```
.  
├── LICENSE  
├── README.md  
├── baselines  
├── bin  
├── detections  
├── docs  
├── investigations  
├── requirements.txt  
├── spec  
├── src  
├── static  
├── stories  
└── venv
```



```
.  
├── app.manifest  
├── appserver  
├── bin  
│   ├── da_ess_contentupdate  
│   ├── da_ess_contentupdate_declare.py  
│   ├── da_ess_contentupdate_declare.pyc  
│   ├── dnstwist.py  
│   ├── escu_contextualize.py  
│   ├── escu_investigate.py  
│   ├── runstory.py  
│   └── splunklib  
├── default  
│   ├── alert_actions.conf  
│   ├── analytic_stories.conf  
│   ├── analyticstories.conf  
│   ├── appsec.conf  
│   ├── collections.conf  
│   ├── commands.conf  
│   ├── content-version.conf  
│   ├── data  
│   ├── distsearch.conf  
│   ├── eventtypes.conf  
│   ├── macros.conf  
│   ├── savedsearches.conf  
│   ├── tags.conf  
│   ├── transforms.conf  
│   ├── ui-tour.conf  
│   ├── usage_searches.conf  
│   └── use_case_library.conf
```

```
#####
# Automatically generated by generator.py in splunk/security-content
# On Date: 2019-07-29T20:54:04 UTC
# Author: Splunk Security Research
# Contact: research@splunk.com
#####
```

```
### ESCU DETECTIONS ###
```

```
[ESCU - AWS Cloud Provisioning From Previously Unseen City - Rule]
```

```
action.escu = 0
```

```
action.escu.enabled = 1
```

```
description = This search looks for AWS provisioning activities from previously unseen cities. Provisioning activities are defined broadly as any event that begins with "Run" or "Create."
```

```
action.escu.mappings = {"cis20": ["CIS 1"], "nist": ["ID.AM"]}
```

```
action.escu.e115 = The subsearch returns all events with event names that start with "Run" or "Create," and then does a 'GeoIP' lookup on the IP address that initiated the action within the last hour. It appends the historical data to those results in the lookup file. Next, it recalculates the 'firstTime' and 'lastTime' field for each country, region, city, and IP address and outputs this data to the lookup file to update the local cache. It then calculates the 'firstTime' and 'lastTime' for each city. It returns only those events from cities that have first been seen in the past hour. This is combined with the main search to return the time, user, IP address, city, event name, and error code from the action.
```

```
action.escu.how_to_implement = You must install the AWS App for Splunk (version 5.1.0 or later) and Splunk Add-on for AWS (version 4.4.0 or later), then configure your CloudTrail inputs. This search works best when you run the "Previously Seen AWS Provisioning Activity Sources" support search once to create a history of previously seen locations that have provisioned AWS resources.
```

```
action.escu.known_false_positives = This is a strictly behavioral search, so we define "false positive" slightly differently. Every time this fires, it will accurately reflect the first occurrence in the time period you're searching with n, plus what is stored in the cache feature. But while there are really no "false positives" in a traditional sense, there is definitely lots of noise.\
```

```
\
This search will fire any time a new city is seen in the **GeoIP** database for any kind of provisioning activity. If you typically do all provisioning from tools inside of your city, there should be few false positives. If you are located in countries where the free version of **MaxMind GeoIP** that ships by default with Splunk has weak resolution (particularly small countries in less economically powerful regions), this may be much less valuable to you.
```

```
action.escu.creation_date = 2018-03-16
```

```
action.escu.modification_date = 2018-03-16
```

```
action.escu.confidence = medium
```

```
action.escu.full_search_name = ESCU - AWS Cloud Provisioning From Previously Unseen City - Rule
```

```
action.escu.search_type = detection
```

```
action.escu.asset_at_risk = AWS Instance
```

```
action.escu.fields_required = []
```

```
action.escu.providing_technologies = ["AWS"]
```

```
action.escu.analytic_story = ["AWS Suspicious Provisioning Activities"]
```

```
cron_schedule = 0 * * * *
```

```
dispatch.earliest_time = -70m@m
```

```
dispatch.latest_time = -10m@m
```

```
action.correlationsearch.enabled = 1
```

```
action.correlationsearch.label = AWS Cloud Provisioning From Previously Unseen City
```

```
action.notable = 1
```

```
action.notable.param.nes_fields = src_ip, city
```

```
action.notable.param.rule_description = Your AWS infrastructure was provisioned from a city, $city$, which has never before been seen provisioning your infrastructure.
```

```
action.notable.param.rule_title = AWS Provision Activity From $city$
```

```
action.notable.param.security_domain = endpoint
```

```
action.notable.param.severity = medium
```

```
action.notable.param.recommended_actions = escu_investigate
```

```
action.notable.param.next_steps = {"version": 1, "data": "Recommended following steps:\n\n1.
```

```
t All AWS Activity From Country\n\nESCU - Get All AWS Activity From Region\n\nESCU - Get All AWS Activity From IP Address\n"} [[action|escu_investigate]]: Based on ESCU investigate recommendations:\n\nESCU - Get All AWS Activity From City\n\nESCU - Ge
```

```
action.risk = 1
```

```
action.risk.param._risk_object = dest
```

```
action.risk.param._risk_object_type = system
```

```
action.risk.param._risk_score = 30
```

```
action.risk.param.verbose = 0
```

```
alert.digest_mode = 1
```

```
alert.suppress = 1
```

```
alert.suppress.fields = dest
```

Why Do This?

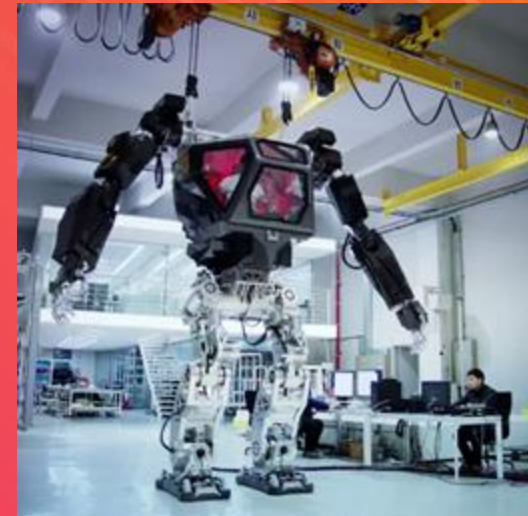
We have a **common schema**, and with a tool we convert json to the actual splunk configurations. We do this because:

1. It is easy to maintain one common spec to generate Splunk **configurations** across multiple projects
2. Splunk savedsearches.conf was not built to define complex detection workflows
3. A common schema allows us to automatically validate and test the content written

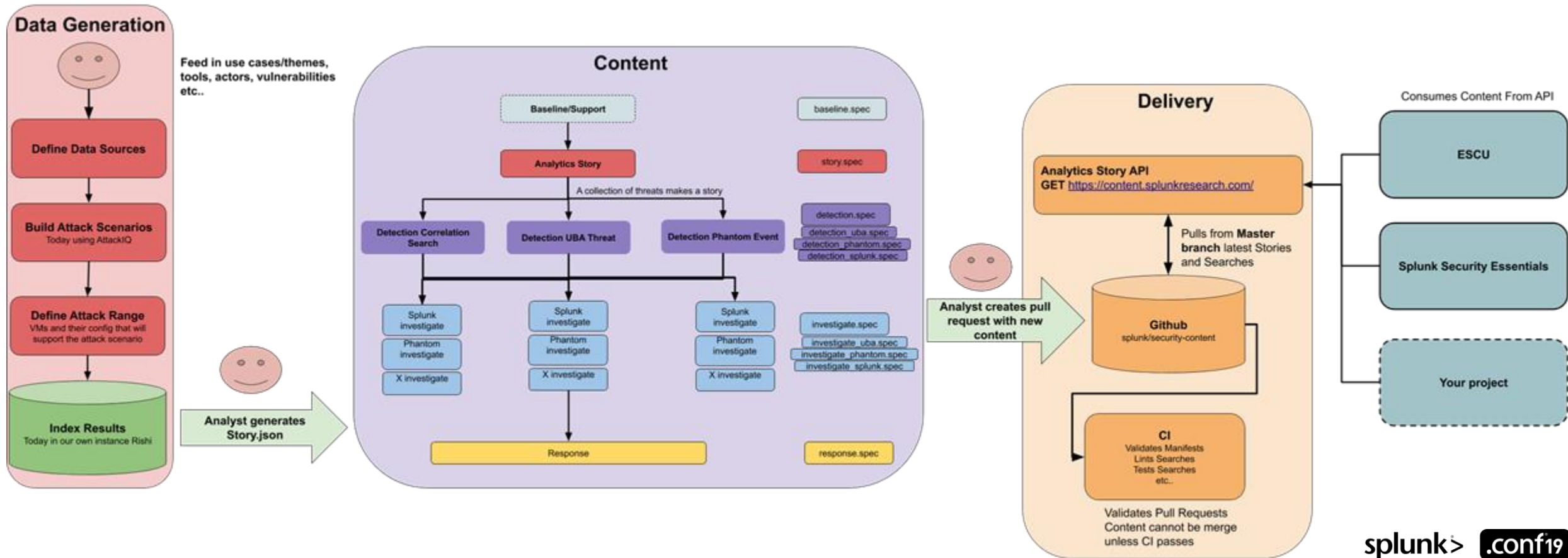


Next Steps

Automating Security Content



How are We Automating Analytic Story Creation?

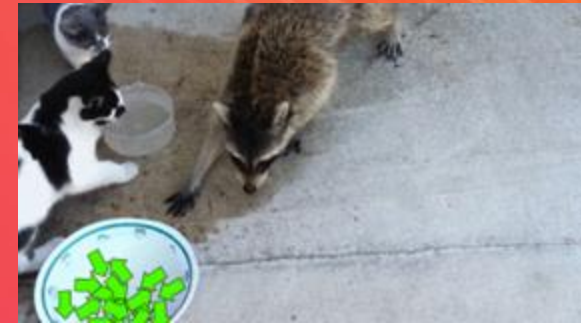




Demo



Key Takeaways



- Splunk can detect, investigate and respond but the content is **spread out** in disparate places
 - **ESCU 2.0** spec brings it all together!
- The specification will allow **new product** content to be easily integrated
- Have **additional information** baked into your security analytics
- **Organize** your security content in one singular place

ESCU App <https://splunkbase.splunk.com/app/3449/>

Analytics Story Execution https://github.com/splunk/analytic_story_execution/



splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION

