© 2018 SPLUNK INC.

Completing the Full OODA Loop

With Symantec, Phantom and Splunk

Colin Gibbens | Director of Product Management

October 2018

© 2018 SPLUNK INC.

Forward-Looking Statements

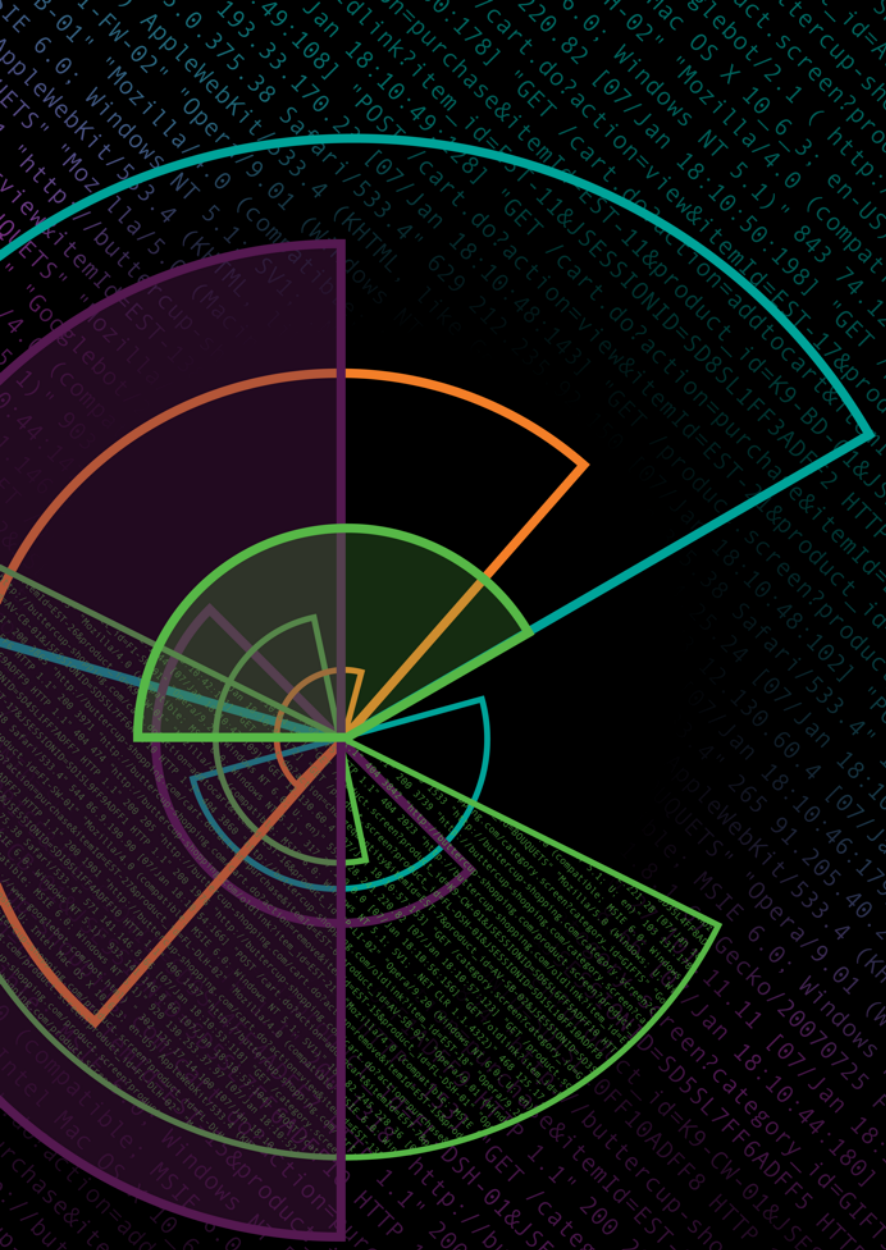
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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. © 2018 Splunk Inc. All rights reserved.

splunk> .conf18

© 2018 SPLUNK INC.

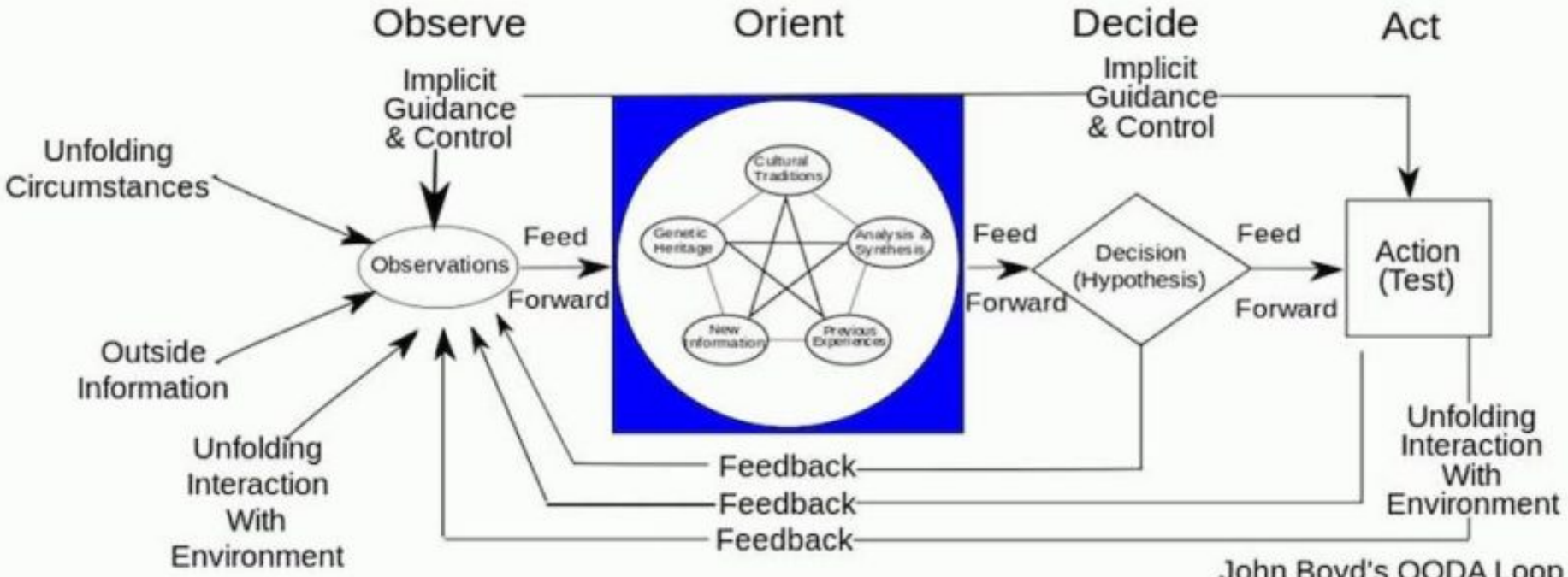


Closing the Loop

The Problem a lot of IR teams face

© 2018 SPLUNK INC.

OODA loop



splunk> .conf18

© 2018 SPLUNK INC.

State of Cyber Defense

Forbes / Tech

DEC 20, 2015 @ 03:01 PM 24,208 VIEWS

Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020

Cybercrime is a growth industry. The returns are great, and the risks are low. We estimate that the likely annual cost to the global economy from cybercrime is more than $400 billion.[1] A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion. Even the smallest

Cybersecurity workforce shortage to reach 1.5 million by 2019.

Mar 24, 2016 | 40 views | 1 Like | 0 Comments

- "The demand for the (cybersecurity) workforce is expected to rise to 6 million (globally) by 2019, with a projected shortfall of 1.5 million" stated Michael Brown, CEO at Symantec, the world's largest security software vendor.

splunk> .conf18

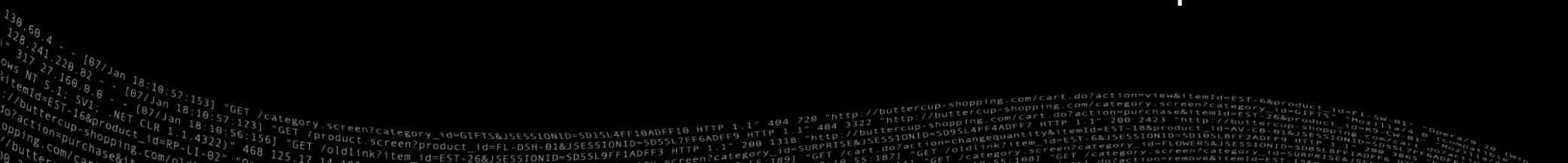
© 2018 SPLUNK INC.

Traditional vs Modern Defense

Traditional Defense

- Prevention is Core
- Mainly Reactive

- **Modern Defense**
- Prevention is ideal but Detection & Response is Crucial
- Detection
  - Having the proper log sources centralized
  - Collecting everything that could have a trace
- Supplementing the SOC with tools that can help them do their job better
- Proactive Threat Hunting
  - Automating enrichment
  - Automating manual task
  - Not depending on a human alone
- OODA Loop



© 2018 SPLUNK INC.

The OODA Loop Consists of Four Parts:

- **Observe** – Decisions are grounded on observations of an evolving circumstance. These observations are the raw data for assessments and actions
- **Orient** – Orientation shapes the way we observe, decide and act Orientation here could be referred to as “tuning.” Filtering and analyzing all the raw data according to rules assists in making decisions and taking action
- **Decide** – From the data observed and filtered, the decision-maker has to select the best possible action
- **Act** – based on your decision, execute your plan

Know when some action is better than no action. If your house is on fire, anything you do to extinguish the blaze is better and then standing and watching it burn. The same applies to a cyberattack

© 2018 SPLUNK INC.

OODA Loop

"Decisions without action are *pointless*
Actions without decisions are **reckless**"

Col. John Boyd

splunk> .conf18

© 2018 SPLUNK INC.

To implement the OODA Loop concept, progressive organizations are using orchestrion as an overlay to their existing security infrastructures. This approach provides the necessary aggregation, intelligence-based analysis, and automation capabilities to identify and respond to cyber threats early in the kill chain.

© 2018 SPLUNK INC.

Blackhat Capture The Flag

- 15 participates
  - 5 highly trained Adversaries (Pen testing, hacking, exploit writing, etc)
- 15 systems setup
  - 3 Linux systems running vulnerable web servers
  - 4 windows (XP, Win 7) systems running POS and ATM software no protection
  - 8 windows (Win 7, 2016, Win 10) systems running web serves, SQL, etc endpoint protection
  - All systems being monitored with EDR
- Canaries (Deceptors) deployed on half the systems
  - Disabled user accounts
  - Fake user accounts with passwords
  - Fake credit card
  - Shares
- Used EDR and FIM to monitor activity on systems and access to canaries
- Main prize $5000 (No winners)
- Smaller prizes based on the number of flags

splunk> .conf18

© 2018 SPLUNK INC.

Attacks

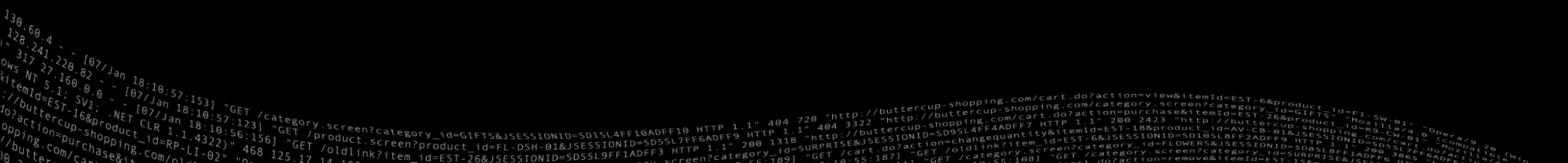
- External Blue against unprotected systems
- Brute force password guessing attacks
- SQL injection
- Mimikatz (Credential dump)
- Directory transversal
- Pass the Hash attacks
- Other exploits
- AD Query

splunk> .conf18

© 2018 SPLUNK INC.

Observe

- Event data I was using to observe what they were doing
  - Windows events logs (logon, logoff, failed logins, RDP logins, etc)
  - Endpoint protection logs (HIPS, Firewall, FIM)
  - EDR events (files accessed, prefetch, smb, rdp)
- Custom Detection Rules
  - Monitor the use of disabled login accounts I created
  - Monitor the access of canaries
  - Lateral movement using RDP or SMB
- Detecting lateral movement and accessing canaries was the biggest key in tracking them
- One of the adversaries made a critical mistake



© 2018 SPLUNK INC.

Orient

- Based on the data I observed I knew I had to act quickly
  - Login attempts with disabled accounts
  - Successful RDP connections to systems that had the flags
  - Access to a canary that I had on one of the systems that had flags
  - Execution of powershell scripts on various systems and the use of credentials
  - Domain admin account stolen and changed
  - Four systems compromised
- Attempted access to one of the main flags
  - Compromised AD server

© 2018 SPLUNK INC.

The Problem

ONE compromised endpoint connected to a corporate domain jeopardizes the entire organization. Attackers can steal domain credentials and by simply querying Active Directory, effortlessly gain full access and visibility to **ALL** servers, applications computers and employees.

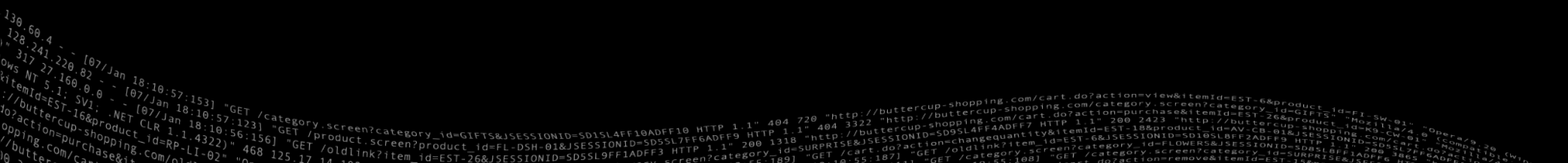
No solution prevents this from happening.

Traditional Active Directory security solutions don't have prevention or analysis capabilities. By the time they detect a breach, attackers have already penetrated the organization.

© 2018 SPLUNK INC.

Decide

- What does this mean to our organization at this time
- What can I do to disrupt the enemy and break his cycle
- Most of my systems are compromised and they have my domain credentials



splunk> .conf18

© 2018 SPLUNK INC.

Act

- Get the system that has the main flags off the network (Isolate)
- Disable the domain admin account
- Block RDP on critical systems
- Push out a policy to block SMB connections
- Push out a policy to blacklist offending IP's

splunk> .conf18

© 2018 SPLUNK INC.

Lessons Learned

- Centralize log data to make the observation and orient phase more streamlined
  - Collect everything that can help observe what is happening in my environment
- Automate and Orchestrate to help deal with the alerts.
  - Remove alerts that are being blocked
  - Enrich the data with asset data so I know what endpoint they are on
  - Enrich the data with user information so I know what user accounts are being accessed
  - Enrich the network traffic with data to let me know who I am dealing with
- Automate and Orchestrate actions
  - Push out actions automatically based on sounded data not just any alert
  - Not all actions do you want to automate you might want a human element to approve

© 2018 SPLUNK INC.

© 2018 SPLUNK INC.

Locard's Exchange Principle

"Every Contact Leaves a Trace"

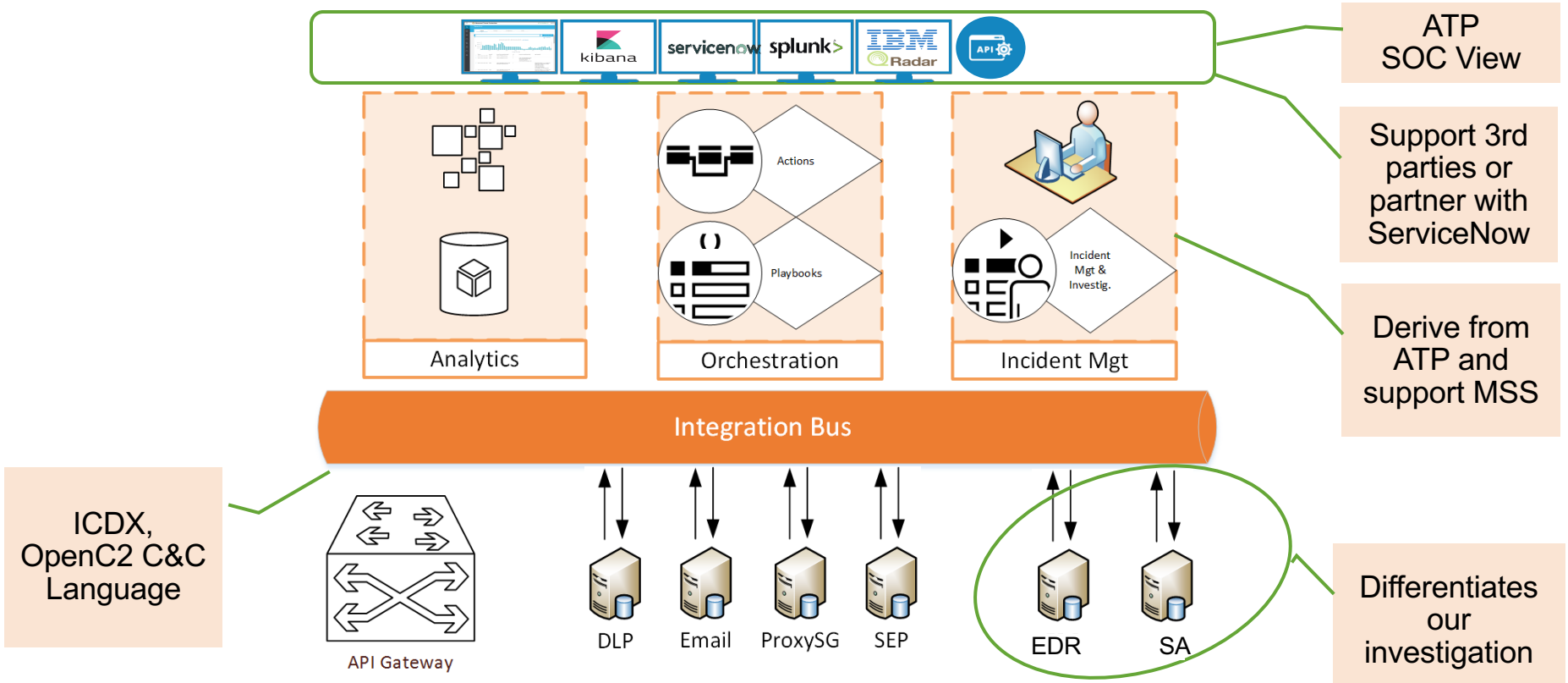
The value of trace (or contact) forensic evidence was first recognized by Edmund Locard in 1910. He was the director of the very first crime laboratory in existence, located in Lyon, France.

The Locard's Exchange Principle states that "with contact between two items, there will be an exchange." For example, burglars will leave traces of their presence behind and will also take traces with them. They may leave hairs from their body or fibers from their clothing behind and they may take carpet fibers away with them.

Source: http://www.virtualsciencefair.org/2004/fren4j0/public_html/trace_evidence.htm

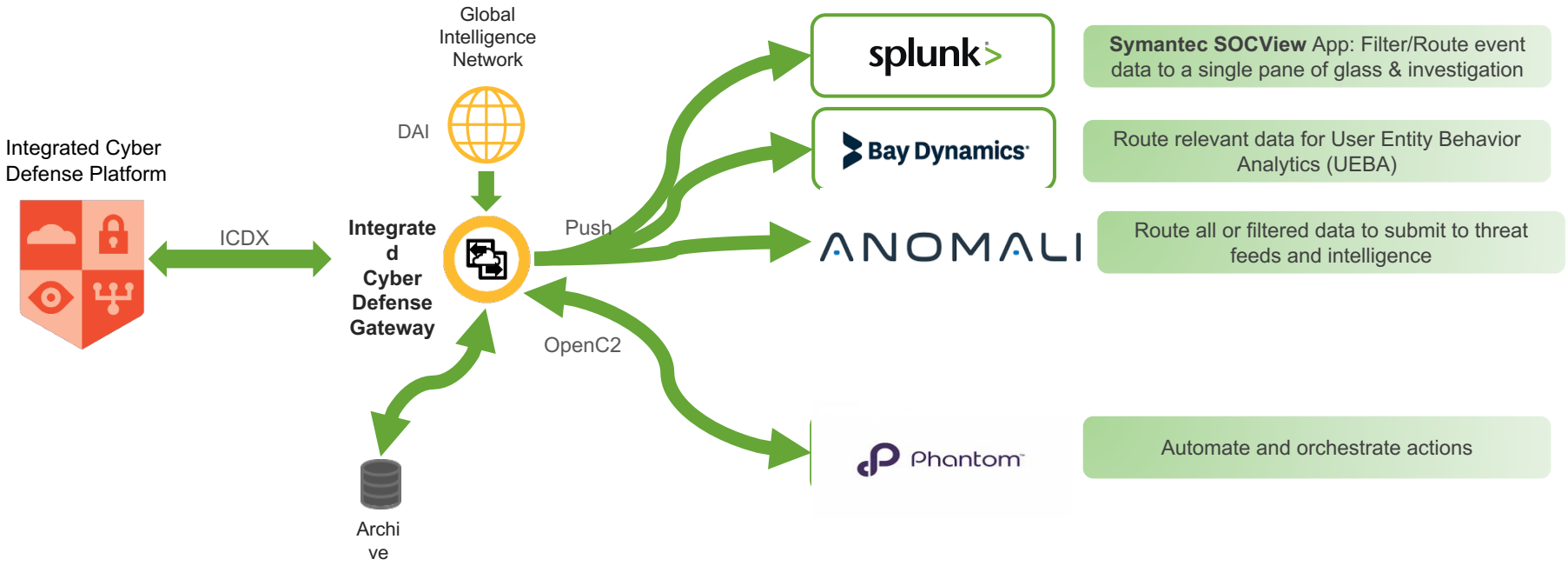
© 2018 SPLUNK INC.

Integrated Cyber Defense | Integration Bus and SOC Workbench



© 2018 SPLUNK INC.

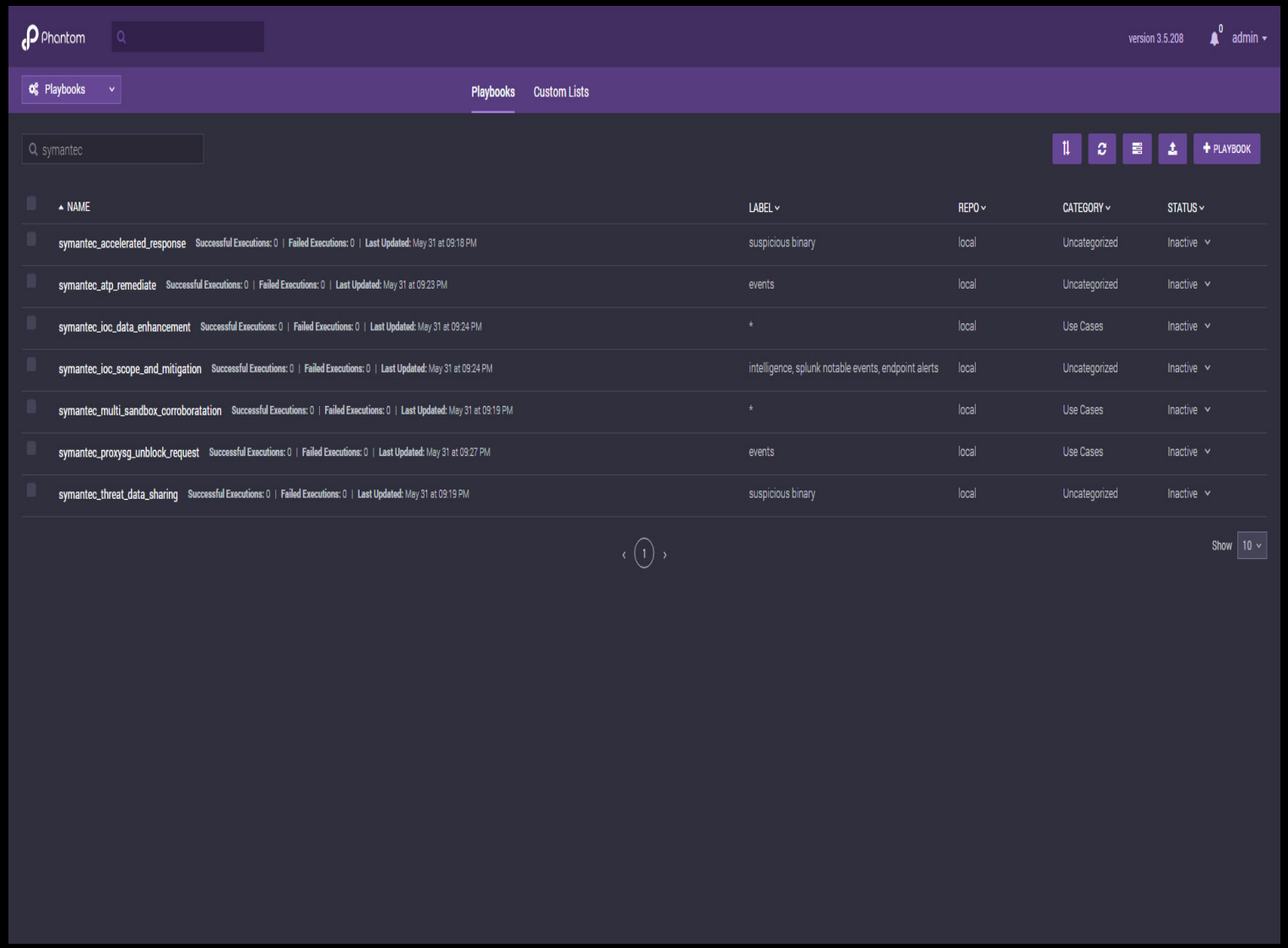
ICDX



© 2018 SPLUNK INC.

Observe

- Observe, which means knowing what's happening on our networks in real time.
- Automate threat intelligent lookups
- Filter out the noise
- We continuously go through the process of gathering data and trying to analyze it

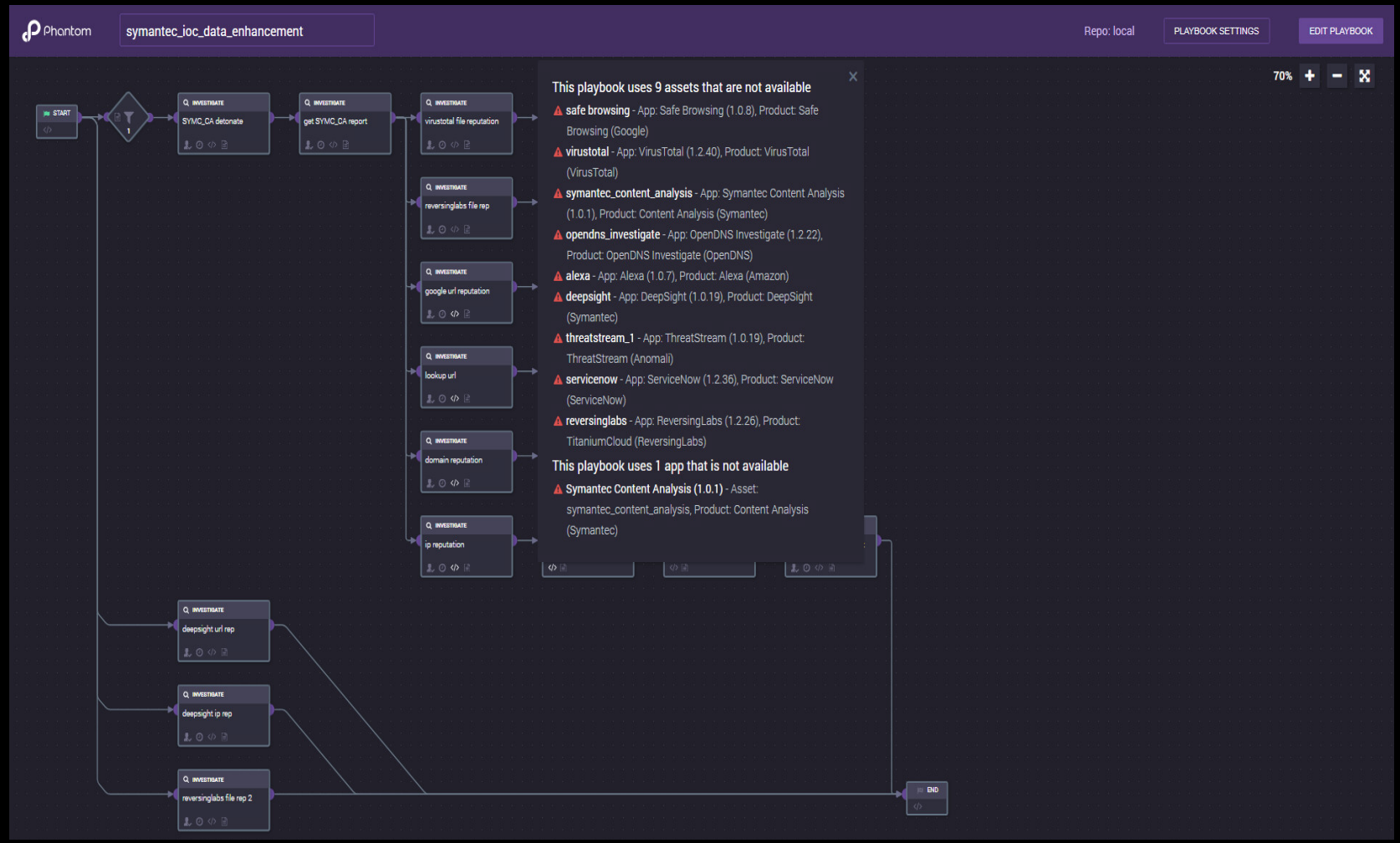


splunk> .conf18

© 2018 SPLUNK INC.

Orient

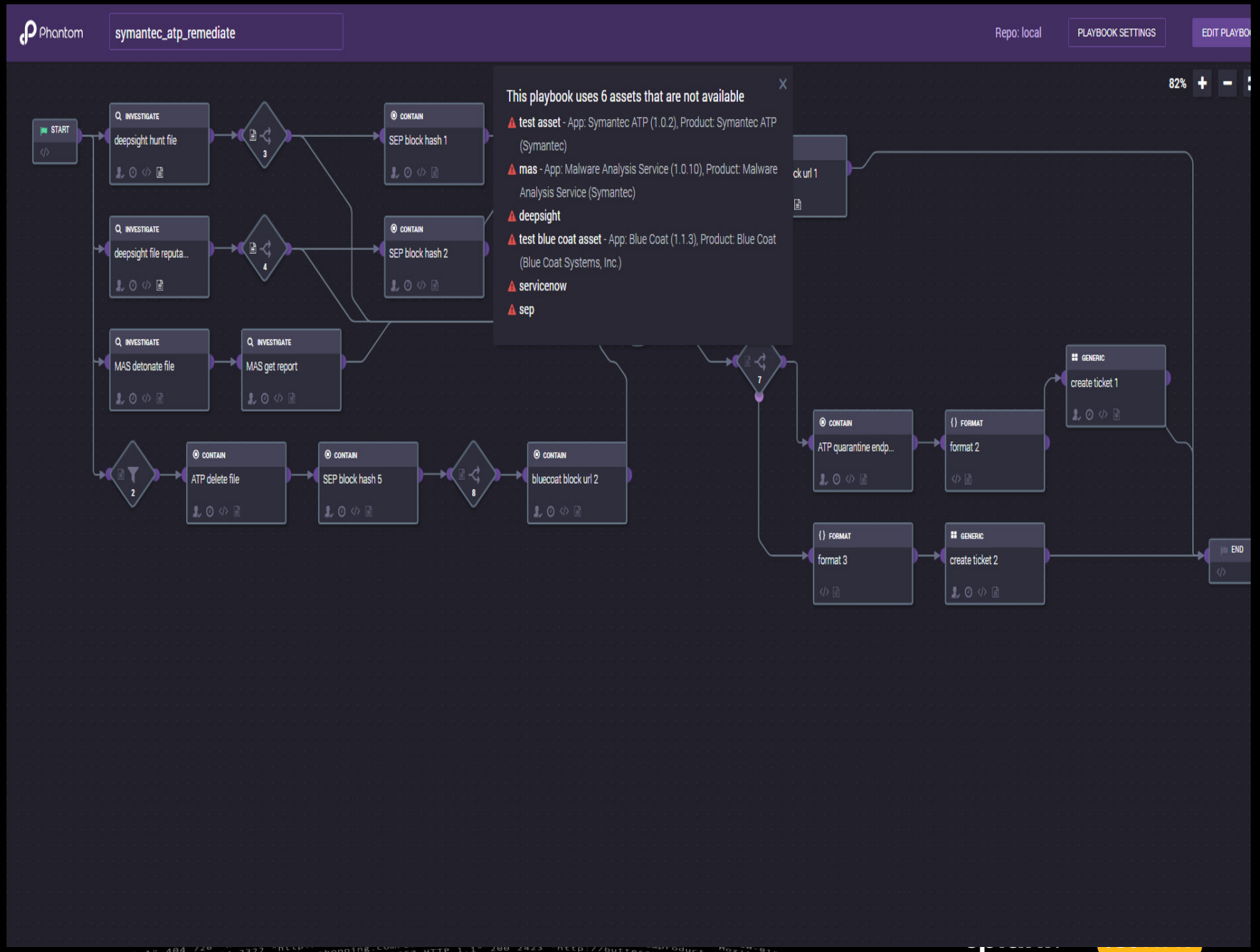
- Orient, which means understanding what it means in context, both in the context of the organization and the context of the greater Internet community. It's not enough to know about the attack; IR teams need to know what it means. Is there a new malware being used by cybercriminals?
- indicators collected from Symantec and third party products are compared against feeds to find artifacts that are traced back to cybercrime groups
- Data enriched from Symantec products can be used to help decide what actions need to be performed



splunk> .conf18

© 2018 SPLUNK INC.

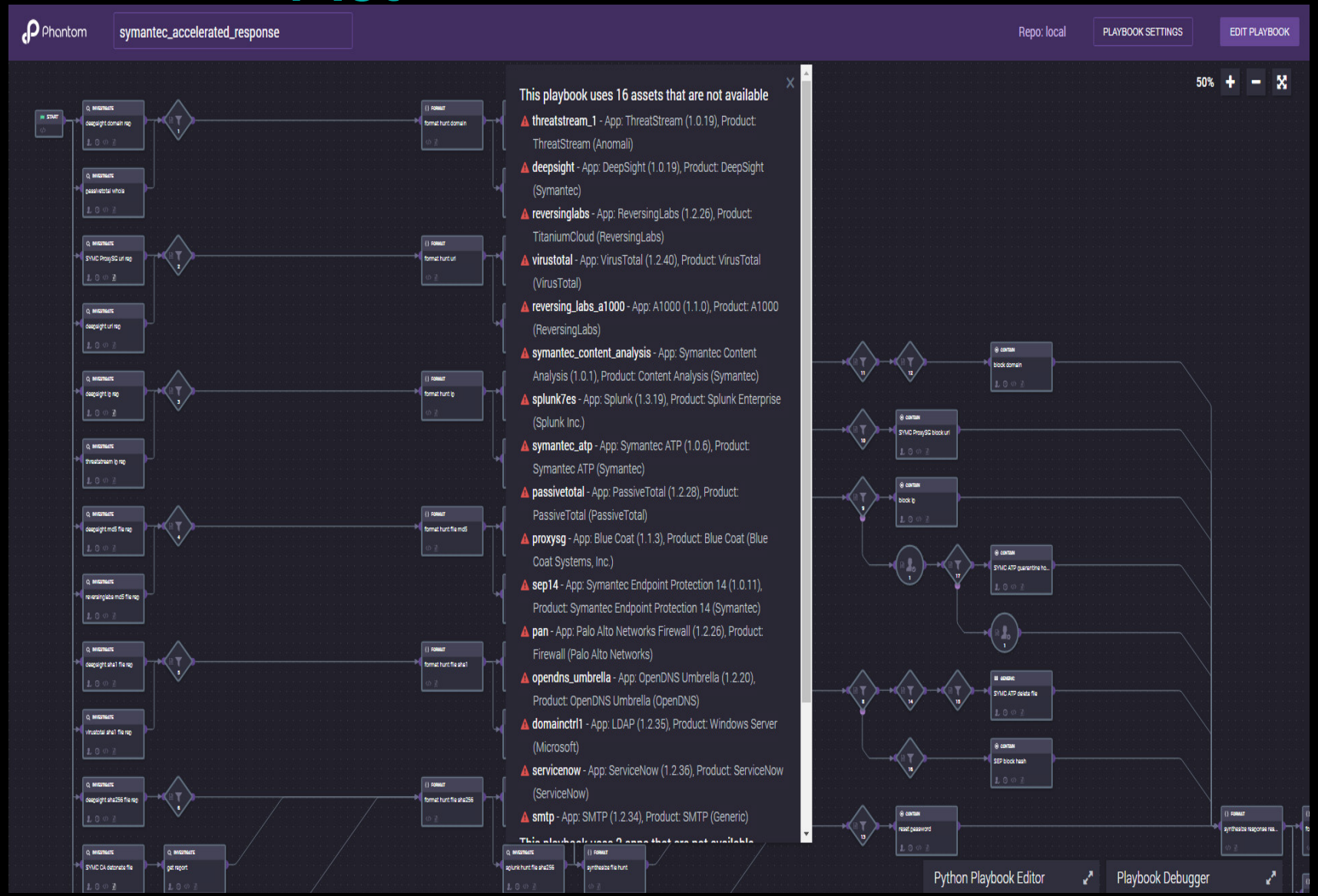
- What does this mean to our organization at this time
- With Phantom it enriches the data with the information we need to be able to decide to act
  - Who
  - What



© 2018 SPLUNK INC.

Act

- With Phantom, Splunk and Symantec you will be able to quickly act on threats targeting your environment and block it across all control points quickly
- Using OODA as a blueprint, it's possible to implement automated processes for pro-active security incident notification and human-guided loop intervention. By establishing thresholds and pre-defined rules, organizations can also orchestrate remediation actions to fix security gaps.



splunk> .conf18

© 2018 SPLUNK INC.

Q&A

Colin Gibbens | Director of Product Mgmt