

DS-19 User Behavior Analytics

Kyle Sweeney, Sabran Evangelista, Jacob Robertson,
Dani Saba, Vimal Raguraman



H4DIPLOMACY



Meet the Team!

Kyle Sweeney, Jacob Robertson,
Sabran Evangelista, Dani Saba,
Vimal Raguraman

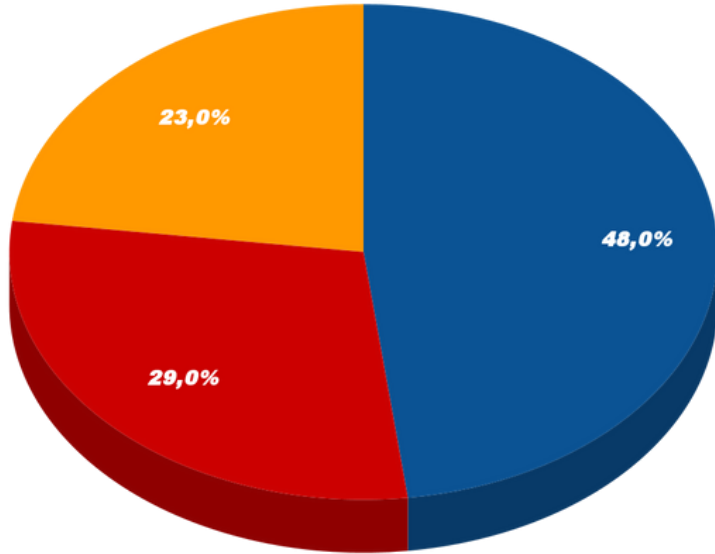
Initial Problem Statement

Network defenders in the Monitoring and Incident Response Division need a more reliable way to detect behavioral anomalies to counter against highly sophisticated cyber attacks by nation state threat actors targeting DOS networks.

Final problem statement

Assist DOS network defenders through **providing tools and/or recommending configurations** that enable the **full functionality of SIEM tools** to identify anomalies in a **centralized data repository**.

Interview Breakdown



Government 46

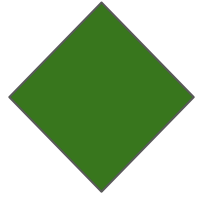
Industry 28

RIT 22

Unique 60

Total 96

Project Journey



Weeks 1-5

Interviews: 8

Days Left: 70

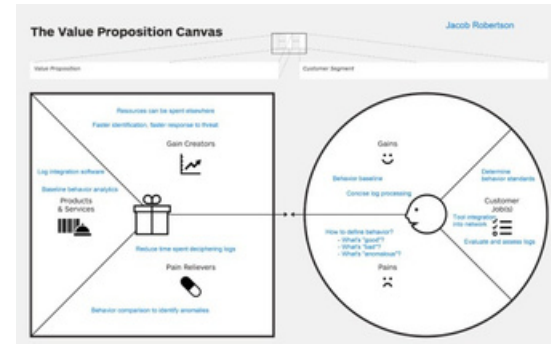
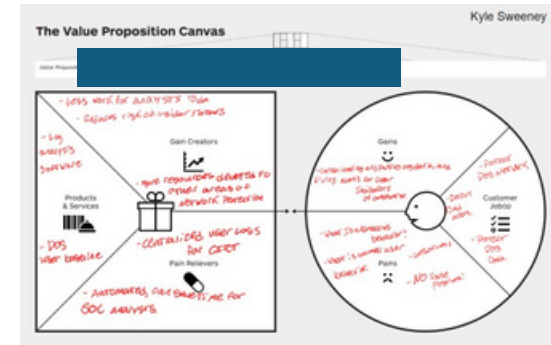
Weeks 1-5

- Total Interviews: 8
 - Met with sponsor to discuss the problem statement
 - Started beneficiary discovery to understand and learn more about the problem domain
 - Broadened scope of problem beyond initial email focus
 - Focus on development of offline algorithm
- Problem Statement:
 - Network defenders in the Monitoring and Incident Response Division need a more reliable way to detect behavioral anomalies to counter against highly sophisticated cyber attacks by nation state threat actors targeting DOS networks.

Weeks 1-5 : Interviews

- Important Interviews:
 - oCIRT Cloud Lead
 - Pivoted away from focusing solely on emails
 - o Unnamed
 - How is network behavior defined? Definitions will not be able to stay static.

Important VPCs



Weeks 1-5 : Mission Model Canvas










The Mission Model Canvas

Mission/Problem Description:
DS-19

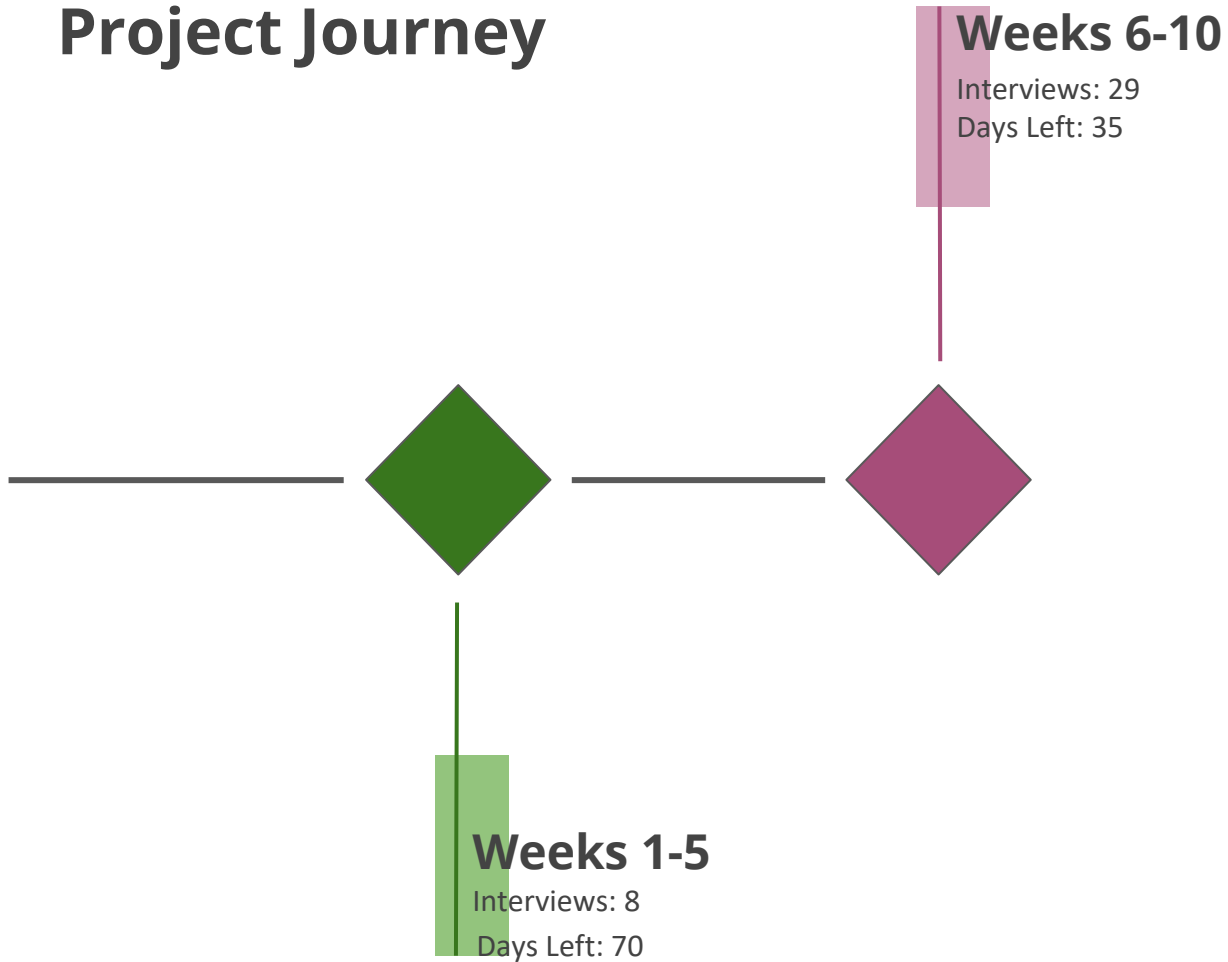
Designed by:

Date:
26 SEP 2023

Version:
3.0

<p>Key Partners </p> <ul style="list-style-type: none">- Danh Nguyen-Huynh - Sponsor- DOS CIRT Team- DOS SOC	<p>Key Activities </p> <p>- Parse data taken from multiple DOS network sources and determine if given user is exhibiting behavior outside of the known norm, indicating identity compromise.</p>	<p>Value Propositions </p> <ul style="list-style-type: none">- Detect anomalous user behavior- Alert SOC once user has shown enough anomalous behavior- Low false positive rate- Consolidated user log information from multiple sources.- DOS user behavior baseline	<p>Buy-in & Support </p> <ul style="list-style-type: none">- Network Defenders- Incident Responders	<p>Beneficiaries </p> <ul style="list-style-type: none">- SOC Analysts- CIRT Analysts- DOS
<p>Mission Budget/Cost </p>	<p>Mission Achievement/Impact Factors </p> <ul style="list-style-type: none">- Detecting and alerting SOC on activity indicative of malicious actor inside network.- prevent bad actors from staying undetected within DOS network.			
<p>Key Resources </p> <ul style="list-style-type: none">- DOS CIRT Team- DOS SOC		<p>Deployment </p> <p>- Offline algorithm that parses logs from multiple data sources and alerts when user behavior deviates from established baseline.</p>		

Project Journey



Weeks 6-10

- Total Interviews: 29
 - Continued meeting with sponsor to understand changes in the problem domain
 - Exploration into Okta-based solution
 - Started looking at Splunk as well
 - How do we define what is good? What is bad?
- Problem Statement Pivot:
 - Assist network defenders in securing DOS network by providing recommended configurations for Splunk and Okta to best utilize these tools to detect bad actors within the DOS network.

Weeks 6-10: Interviews

➤ Important Interviews:

oOkta Internal Meeting

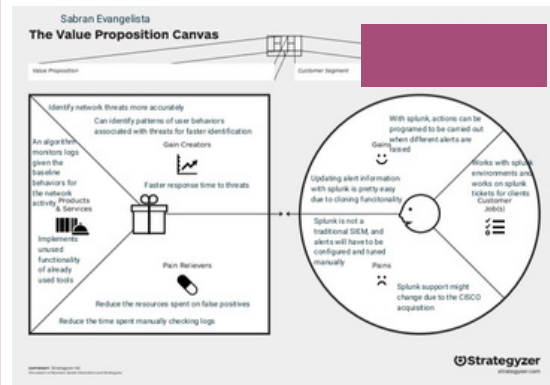
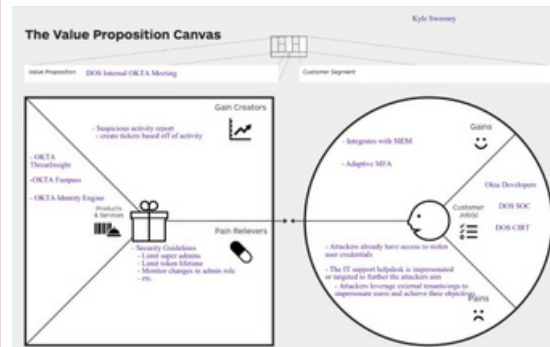
- Learned a lot about existing Okta provided solutions and more about DoS security practices

o

- Provided a lot of insight as to how Splunk works with alerting and logging information

“The big question to answer will be how you define good and bad events”

Important VPCs



Weeks 6-10 : Mission Model Canvas

The Mission Model Canvas

Mission/Problem Description:

DS-19








Designed by:

Date:

24 OCT 2023

Version:

5.0

<p>Key Partners </p> <ul style="list-style-type: none"> - Danh Nguyen-Huynh - sponsor - DOS Cirt - [Redacted] - DOS SOC - Okta Dev Team - Splunk Dev Team 	<p>Key Activities </p> <ul style="list-style-type: none"> - Construct list of recommended Okta and Splunk configurations to best use existing tools within the DOS network. - Increase volume and verbosity of log event data to better assist incident response 	<p>Value Propositions </p> <ul style="list-style-type: none"> - Strengthen more vulnerable parts of the network due to increased analyst bandwidth - Better inform incident response decisions - Increased volume of valuable event log data assist CIRT in resolving incidents - Reduce/reallocate personnel assigned to cloud monitoring - Utilizes government approved tools, saves hassle of government approval process - Increase DOS data and network security 	<p>Buy-in & Support </p> <ul style="list-style-type: none"> - Reduces manpower needed to review logs, can allocated elsewhere - Reduces time between detecting actor and removing credentials - Consolidates information in time-sensitive situation - Reduce DOS secrets leaking 	<p>Beneficiaries </p> <ul style="list-style-type: none"> - SOC Analysts - CIRT Analysts - [Redacted] - DOS Cyber Monitoring and Operations
<p>Mission Budget/Cost </p> <p>Currently Unknown</p>		<p>Mission Achievement/Impact Factors </p> <ul style="list-style-type: none"> - Reduce time between network compromise and credential revocation by X - Present relevant information to CIRT to reduce work time lost due to false positives by X - Reduce # of DOS annual network breaches by x% 		

1st MVP

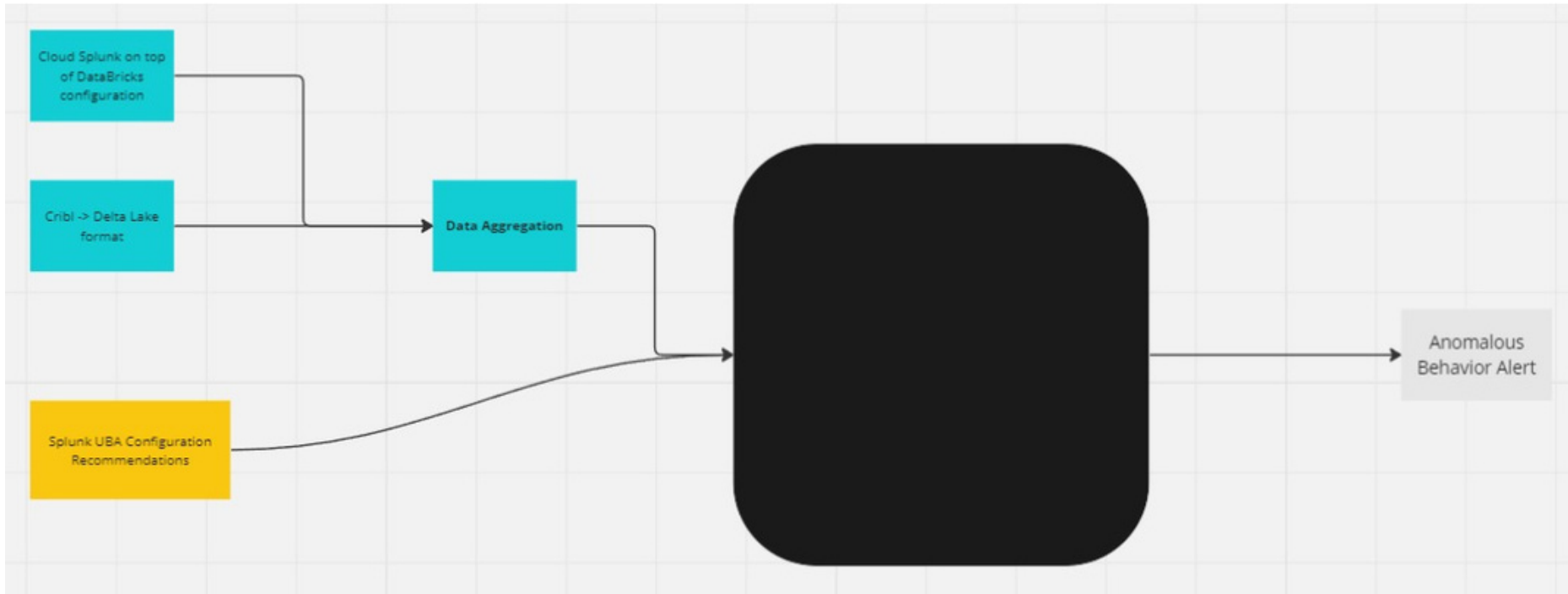
Okta Configuration
Recommendations

Splunk UBA Configuration
Recommendations

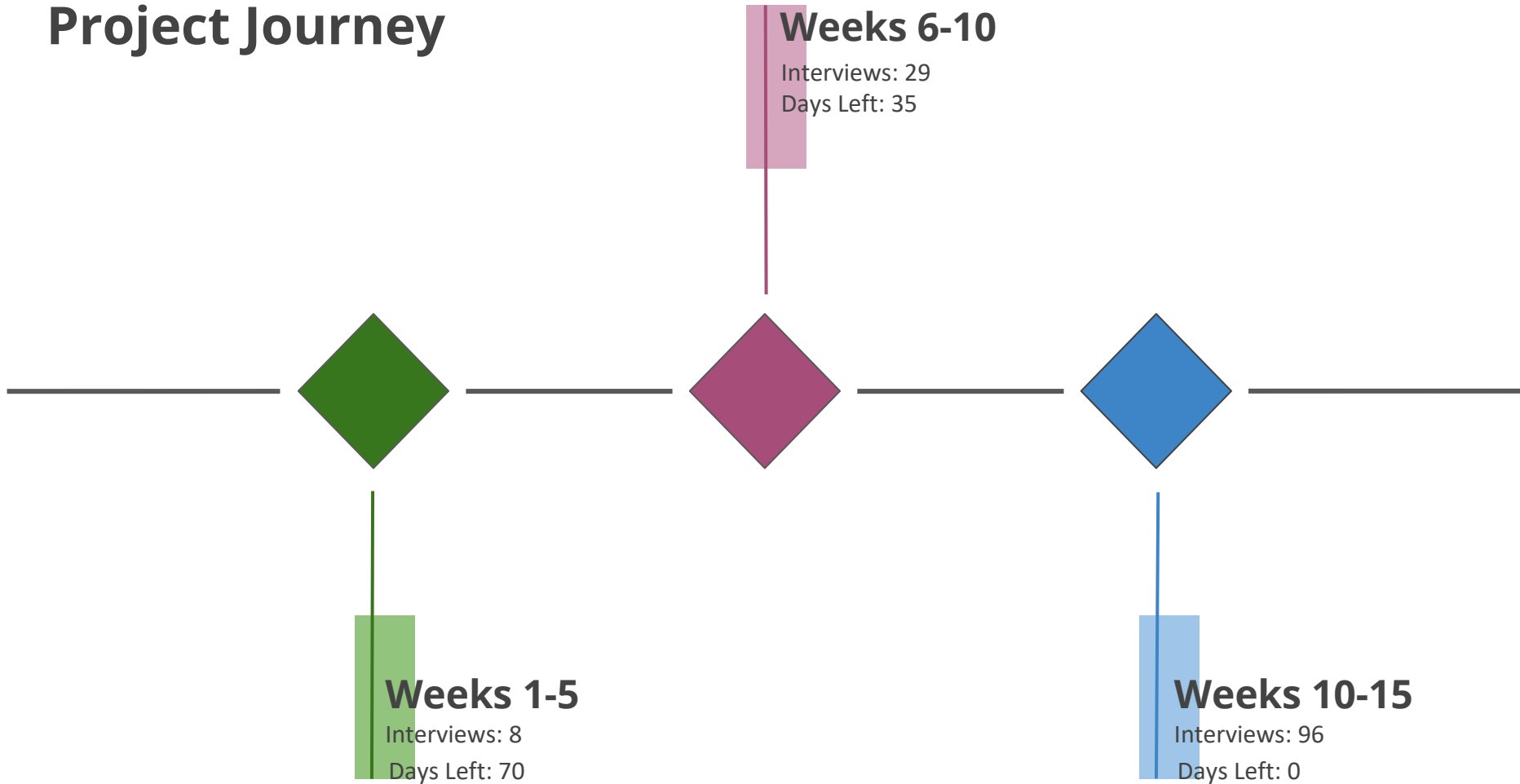


Anomalous
Behavior Alert

2nd MVP



Project Journey



Weeks 6-10

Interviews: 29
Days Left: 35

Weeks 1-5

Interviews: 8
Days Left: 70

Weeks 10-15

Interviews: 96
Days Left: 0

Weeks 10-15

- Total Interviews: 96
 - Went down to Washington D.C. to gather more crucial information for the problem domain
 - Pivoted away from Okta, and configuration recommendations
 - Began focusing on a SIEM centered solution
 - More thought into creating a tool agnostic solution/framework
- Final Pivot:
 - Assist DOS network defenders through providing tools and/or recommending configurations that enable the full functionality of SIEM tools to identify anomalies in a centralized data repository.

Weeks 10-15: Interviews

➤ Important Interviews:

oDOS IT Specialist

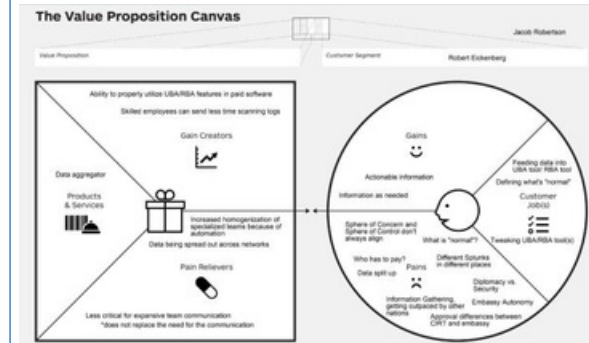
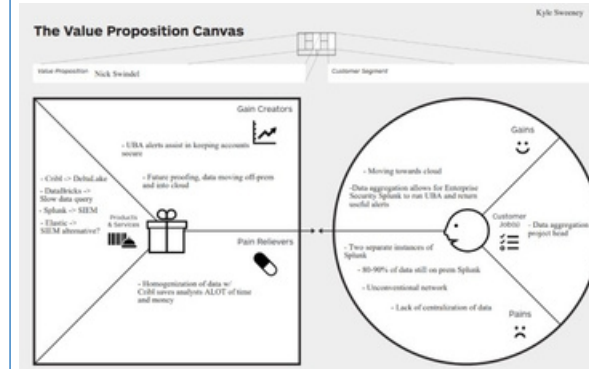
■ Got an overview of the DoS network and how they are utilizing Splunk

oDOS Branch Chief

■ Highlighted several issues both technical and non-technical that opened up the problem space

“Don’t let a good crisis go to waste”
-DOS Branch Chief

Important VPCs



Weeks 10-15 : Mission Model Canvas



The Mission Model Canvas

Mission/Problem Description:
DS-19

Designed by:

Date:
28 NOV 2023

Version:
8.0

<p>Key Partners </p> <ul style="list-style-type: none"> - Danh Nguyen-Huynh - sponsor - DoS CIRT - [Redacted] - DoS SOC - DoS CMO - [Redacted] 	<p>Key Activities </p> <ul style="list-style-type: none"> - Aggregate data from across full DoS network, homogenize data format to DeltaLake using Cribl, query slow storage using data lake/DataBricks. - Move Enterprise Security License to cloud Splunk instance - Run Splunk UBA tools on aggregated DoS dataset and return alerts to FACC CIRT 	<p>Value Propositions </p> <ul style="list-style-type: none"> - Strengthen vulnerable parts of DoS network due to increased analyst bandwidth - Better informed incident response decisions - Increased volume of valuable UBA log data to assist CIRT in detection and resolution of incidents - Utilizes government approved tools, saves hassle of government approval process - Increase effectiveness of CIRT analysts through UBA alerts - Increase DoS Data and network security - Data aggregation from all sources across highly unconventional network structure 	<p>Buy-in & Support </p> <ul style="list-style-type: none"> - Reduces manpower needed to review logs, can be allocated elsewhere - Reduces time between detecting actor and removing credentials - Data aggregation from across entire uneven DoS network. - Consolidate information in time-sensitive situation - Automation of data formatting across various data sources - Reduce DoS secrets leaking 	<p>Beneficiaries </p> <ul style="list-style-type: none"> - SOC Analysts - CIRT Analysts - [Redacted] - Lead CIRT Cloud Analyst - [Redacted] - CIRT Cloud Lead - [Redacted] - CIRT Team Lead - DoS Cyber Monitoring and Operations - [Redacted] - IT Specialist - [Redacted] - Consultant - [Redacted] - CIRT Department Head - [Redacted] - Engineering Department Head
<p>Mission Budget/Cost </p> <p>\$4.6 Million yearly to run ES Splunk on cloud with 10TB a day \$1.1 for ES Splunk License DataBricks -> \$0.55 per DBU/hour Cribl -> ~\$120k yearly for 1TB/day</p>		<p>Mission Achievement/Impact Factors </p> <ul style="list-style-type: none"> - Reduce SOC alert false positive rate by 50% - Reduce time between network compromise and credential revocation by 70% 		

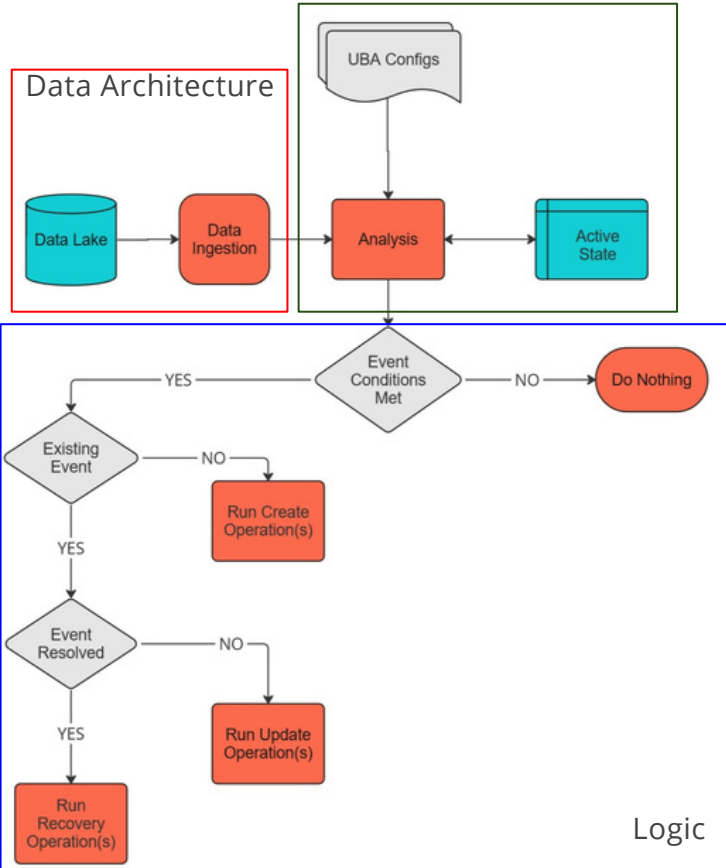


DC Trip!

Left to Right: Sabran, Kyle, Jacob, Danh
(Problem Sponsor)

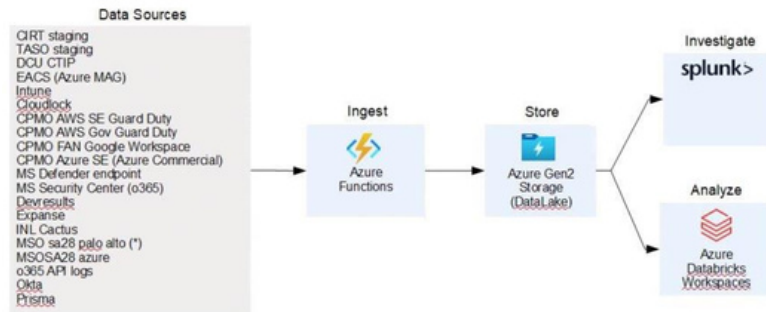
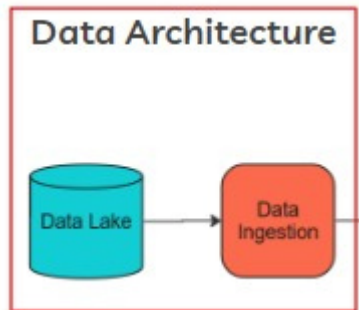
Final MVP

Analysis



Data Architecture

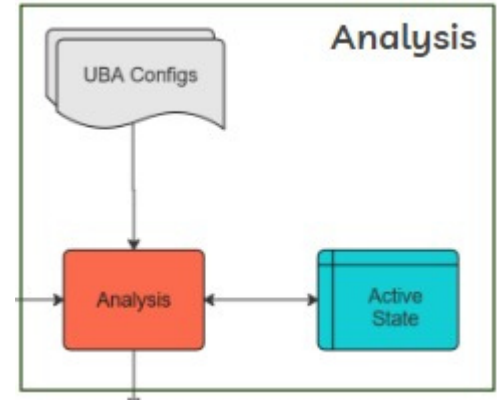
- DS-6 Data Architecture for Cybersecurity
 - o Uneven network/data structure
- Normalizer
 - o Cribl -Delta Lake
- Data Lake
 - o Data Hub + Data Nodes
- Splunk ES Cloud
 - o Databricks
- Interaction with cold storage



Analysis

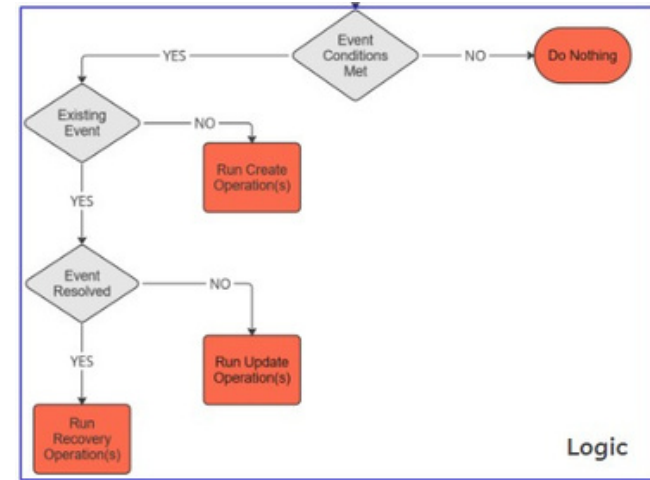
- Triggers
 - Defined by the configurations of the UBA tool
 - Pulled based off of data from a user state database

- Active State
 - Define “normal” user behavior
 - Working hours, access patterns, etc.
 - Fingerprint users outside of IP



Logic

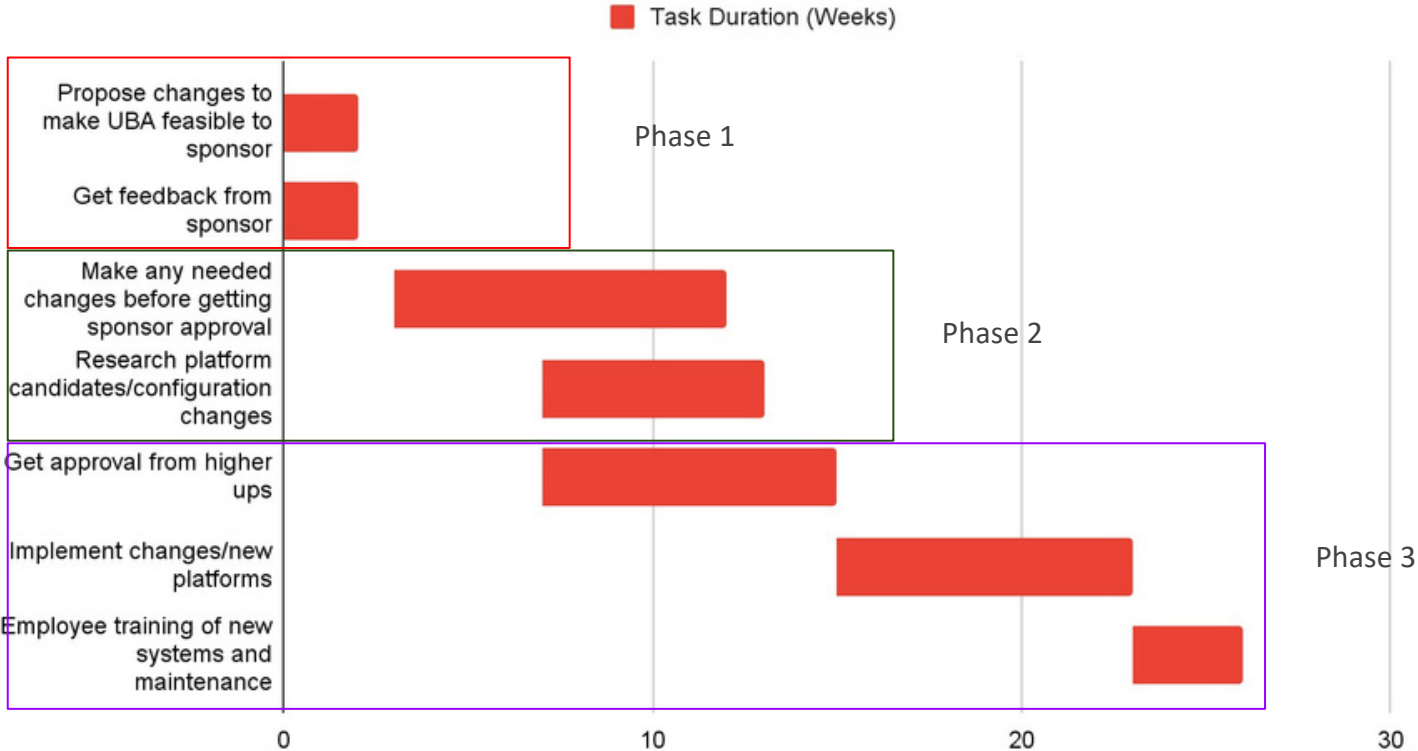
➤ How to respond when a Trigger has been pulled?
Alerts? Run Commands? Shut off access?



➤ Operations

- Act in accordance with situational factors
 - User Privilege
 - Persistence of the Event

Gantt Chart



Thank You!

Special thank you to Jim Santa, Suvam Barui, Danh Nguyen-Huynh, and Danny Potocki!

Thank you to everyone who we interviewed!



Questions?