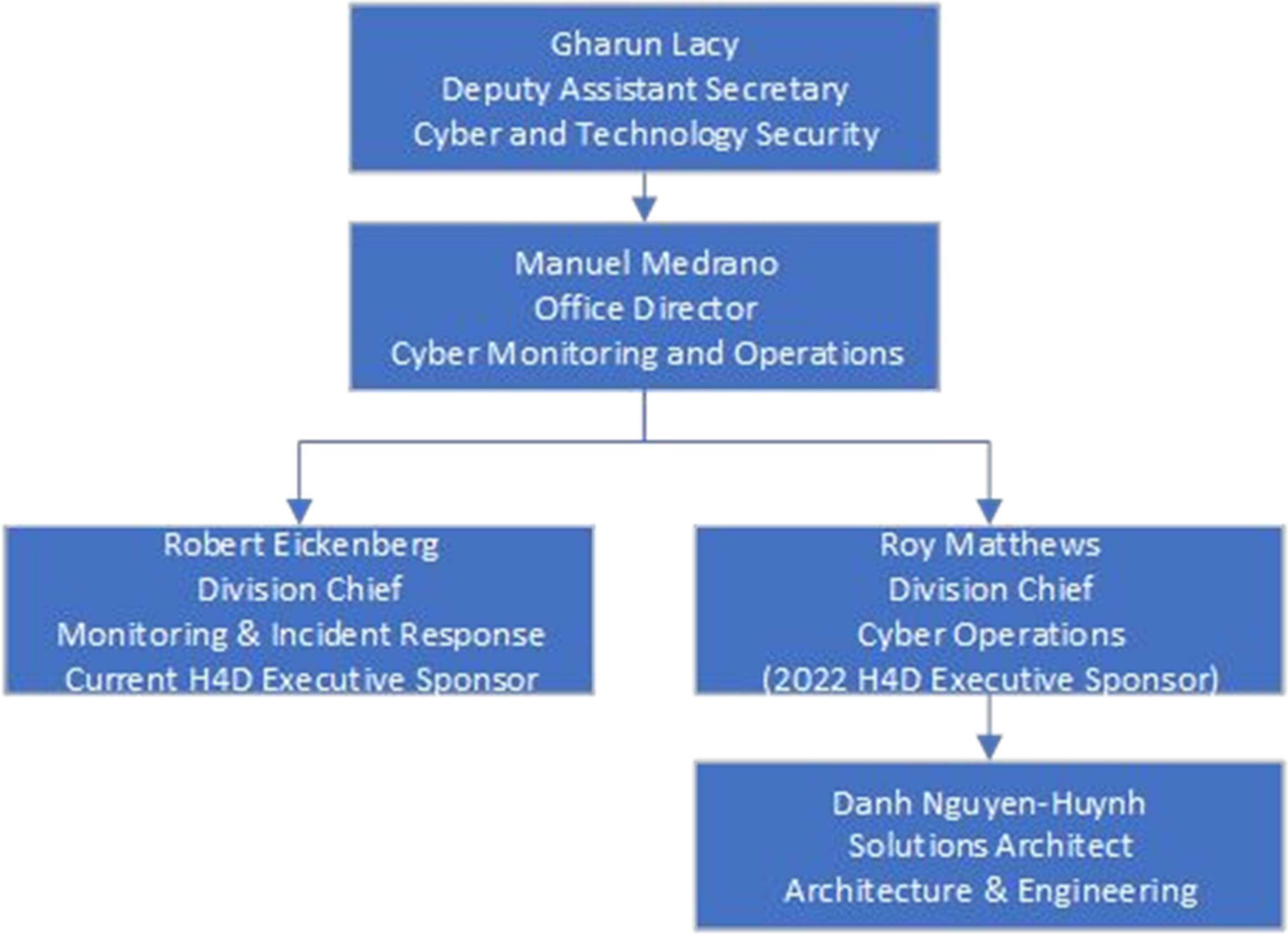
DS-19 Week 6

Kyle,Sabran,Jacob,Dani,Vimal

Interviews Completed: 14
Scheduled: 4



Gharun Lacy
Deputy Assistant Secretary
Cyber and Technology Security

Manuel Medrano
Office Director
Cyber Monitoring and Operations

Robert Eickenberg
Division Chief
Monitoring & Incident Response
Current H4D Executive Sponsor

Roy Matthews
Division Chief
Cyber Operations
(2022 H4D Executive Sponsor)

Danh Nguyen-Huynh
Solutions Architect
Architecture & Engineering

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.

Assist network defenders in securing DOS network by utilizing Okta log data and DOS user behavior baseline to detect bad actors within DOS network.

The Mission Model Canvas

Mission/Problem Description: DS-19

Designed by:

Date: 3 OCT 2023

Version: 4.0

Key Partners

- [redacted]
- DOS CIRT

[redacted]

- DOS SOC
- Okta dev team

Key Activities

- Gather user behavior data from Okta and Splunk logs
- Compare log data to behavior baseline to determine network compromise
- Present relevant information to CIRT to inform decision to pull back credentials

Key Resources

- $x for algorithm creation
- Okta/Splunk log data(expanding coverage)
- Lots of DOS user data to develop user baseline
- ML for user baseline

Value Propositions

- Low false positive rate
- Automated internal threat detection
- Strengthen more vulnerable parts of network due to increased bandwidth
- User behavior report
- Inform incident response decisions
- Increase DOS data and network security
- Reduce/reallocate personnel assigned to cloud monitoring

Buy-in & Support

- Reduces manpower needed to review logs, can be allocated elsewhere
- Reduces time between detecting actor and removing credentials
- Consolidates information in time-sensitive situation
- Reduce DOS secrets leaking

Deployment

- Alerts from algorithm to SOC notifying of anomalous user behavior within network
- User behavior report for post-incident action
- UI....

Beneficiaries

- SOC Analysts
- CIRT Analysts

[redacted]

- DOS Cyber Monitoring and Operations

Mission Budget/Cost

Currently unknown

Mission Achievement/Impact Factors

- 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%

DESIGNED BY: Strategyzer AG & Steve Blank
The makers of Business Model Generation and Strategyzer

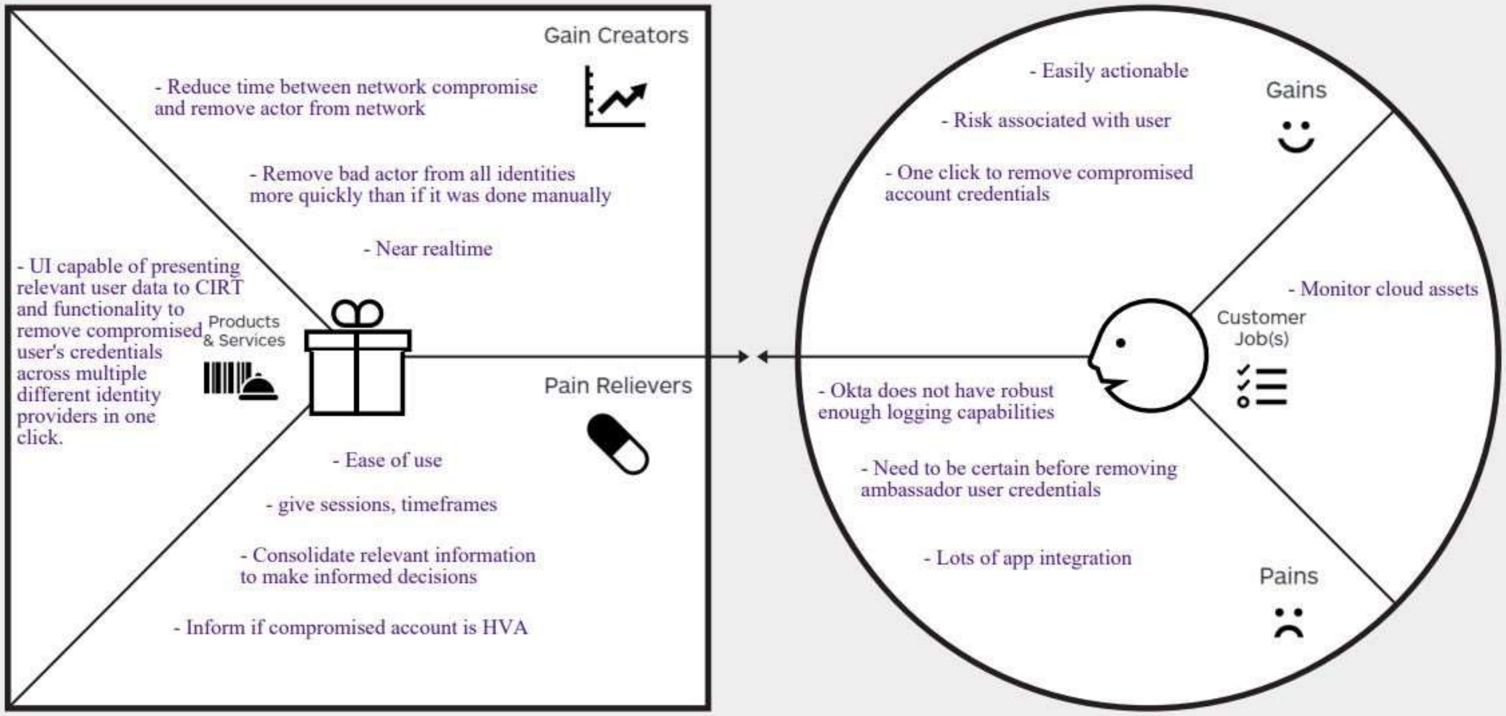
Strategyzer
strategyzer.com

The Value Proposition Canvas

Kyle Sweeney

Value Proposition [redacted]

Customer Segment



Gain Creators

- Reduce time between network compromise and remove actor from network

- Remove bad actor from all identities more quickly than if it was done manually

- Near realtime

Products & Services

- UI capable of presenting relevant user data to CIRT and functionality to remove compromised user's credentials across multiple different identity providers in one click.

Pain Relievers

- Ease of use

- give sessions, timeframes

- Consolidate relevant information to make informed decisions

- Inform if compromised account is HVA

Gains

- Easily actionable

- Risk associated with user

- One click to remove compromised account credentials

Customer Job(s)

- Monitor cloud assets

Pains

- Okta does not have robust enough logging capabilities

- Need to be certain before removing ambassador user credentials

- Lots of app integration

Strategyzer
strategyzer.com

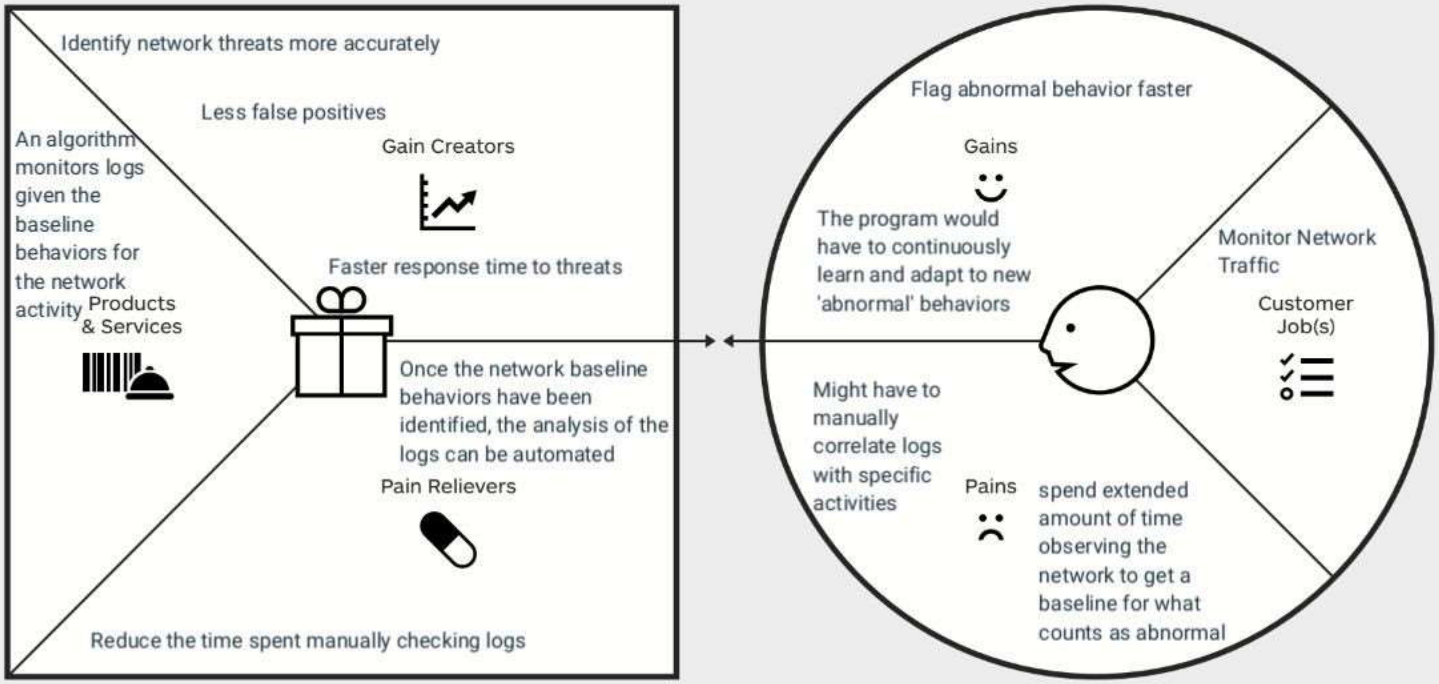
Sabran Evangelista

The Value Proposition Canvas

Interview with [redacted]
Principle Lecturer at RIT

Value Proposition

Customer Segment



Identify network threats more accurately

Less false positives

Gain Creators

An algorithm monitors logs given the baseline behaviors for the network activity

Products & Services

Faster response time to threats

Once the network baseline behaviors have been identified, the analysis of the logs can be automated

Pain Relievers

Reduce the time spent manually checking logs

Flag abnormal behavior faster

Gains

The program would have to continuously learn and adapt to new 'abnormal' behaviors

Monitor Network Traffic

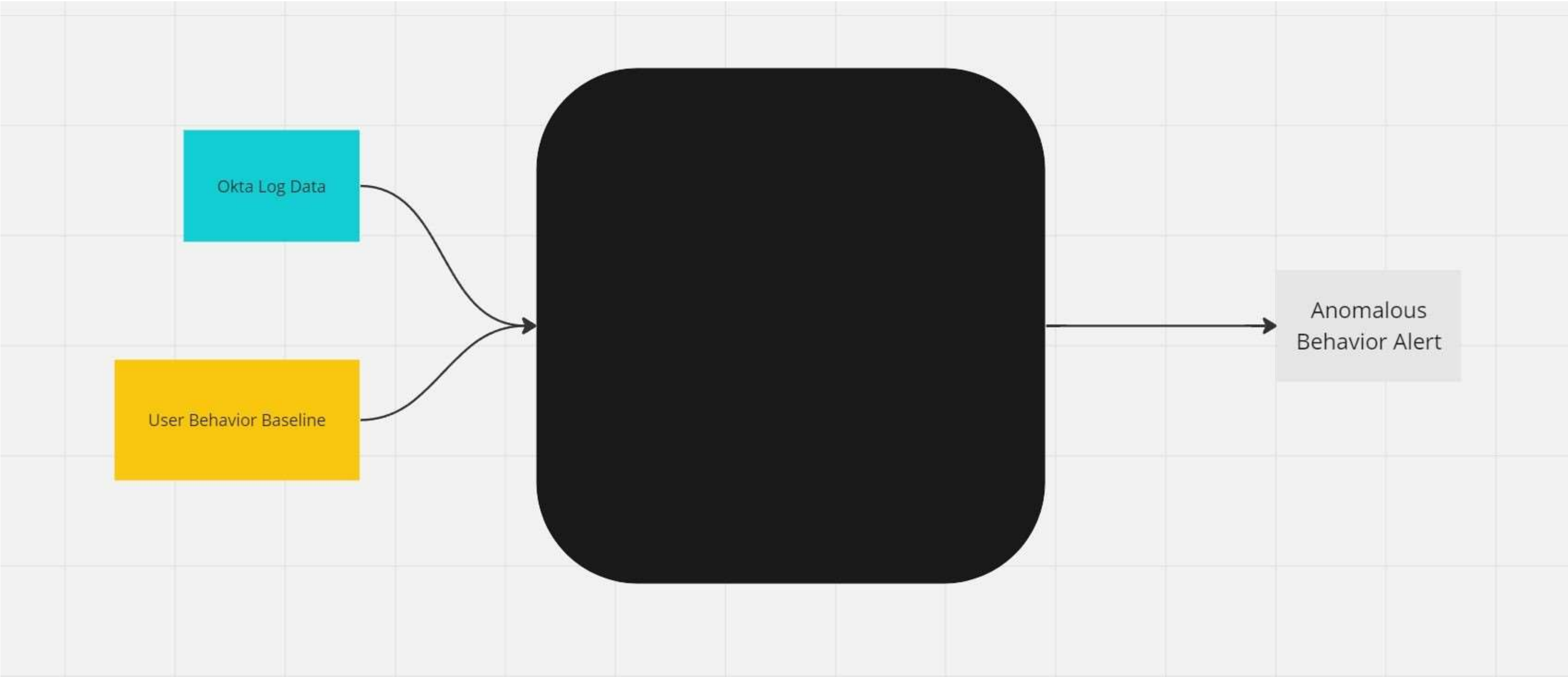
Customer Job(s)

Might have to manually correlate logs with specific activities

Pains

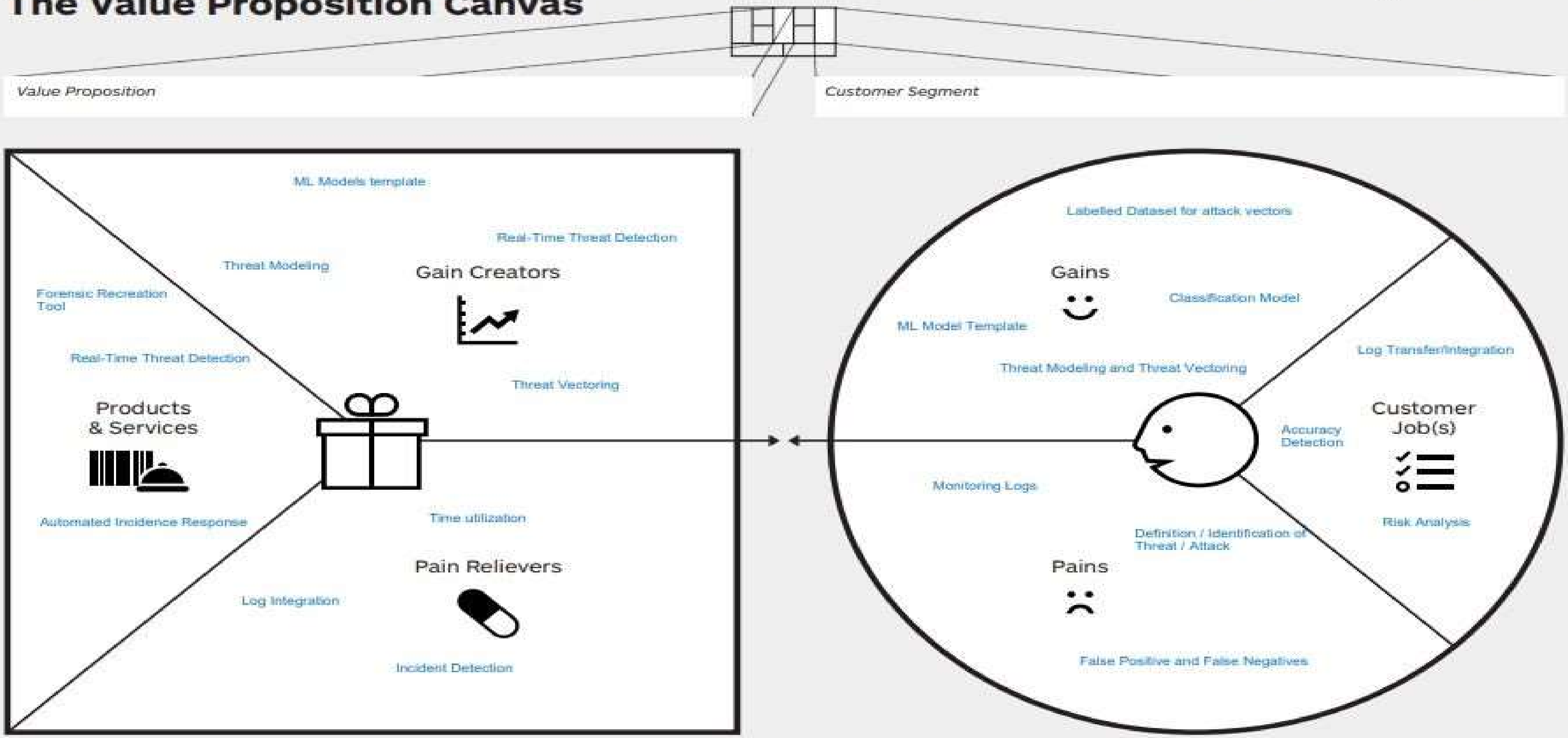
spend extended amount of time observing the network to get a baseline for what counts as abnormal

Strategyzer
strategyzer.com


Okta Log Data
User Behavior Baseline
Anomalous Behavior Alert

The Value Proposition Canvas

Vimal Seshadri Raguraman



Value Proposition

Customer Segment

Gain Creators

ML Models template

Real-Time Threat Detection

Threat Modeling

Threat Vectoring

Products & Services

Forensic Recreation Tool

Real-Time Threat Detection

Automated Incidence Response

Pain Relievers

Time utilization

Log Integration

Incident Detection

Gains

Labelled Dataset for attack vectors

Classification Model

ML Model Template

Threat Modeling and Threat Vectoring

Customer Job(s)

Log Transfer/Integration

Accuracy Detection

Risk Analysis

Pains

Monitoring Logs

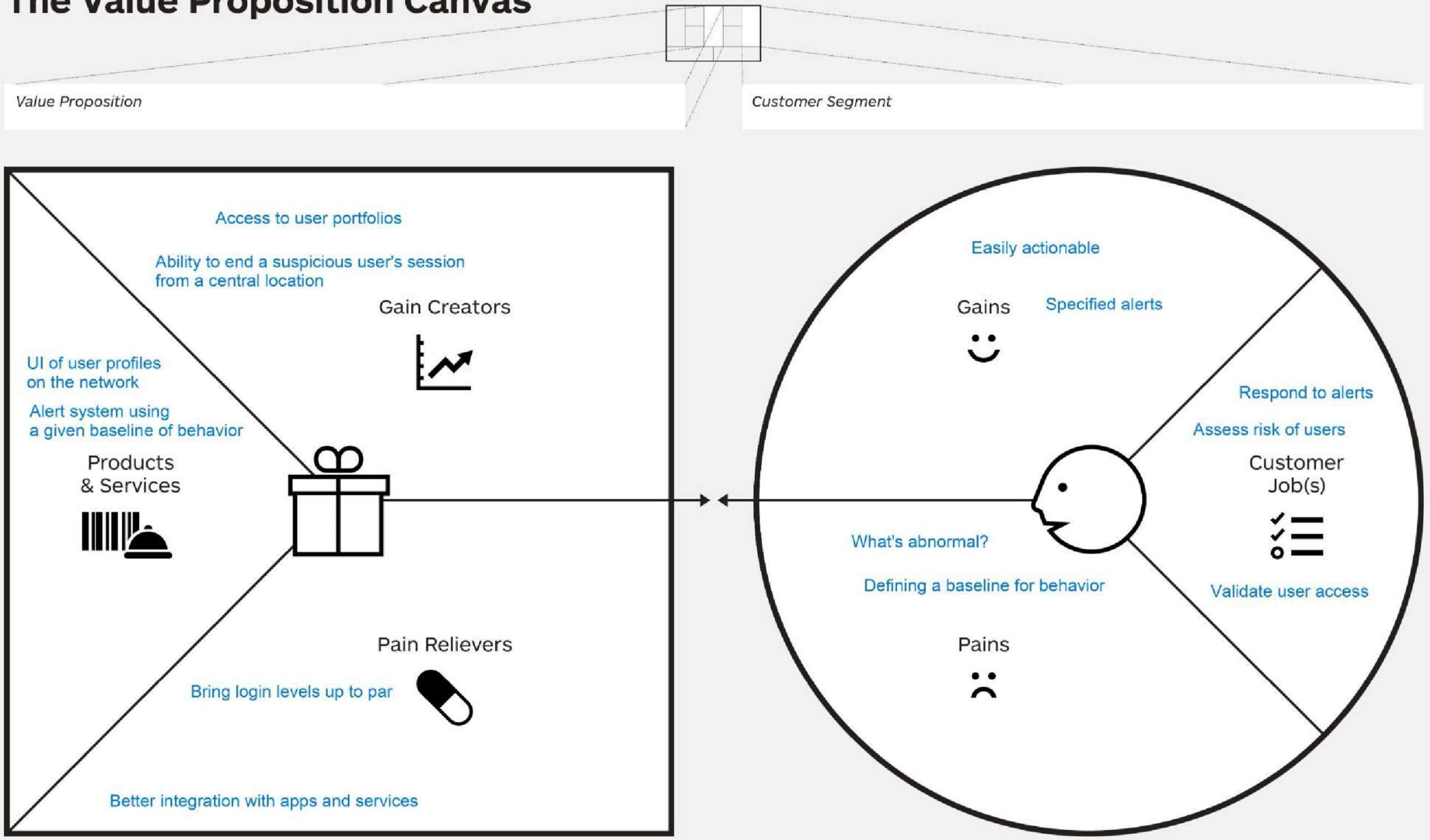
Definition / Identification of Threat / Attack

False Positive and False Negatives

Strategyzer
strategyzer.com

The Value Proposition Canvas

Jacob Robertson



Value Proposition

Gain Creators

Access to user portfolios

Ability to end a suspicious user's session from a central location

Products & Services

UI of user profiles on the network

Alert system using a given baseline of behavior

Pain Relievers

Bring login levels up to par

Better integration with apps and services

Customer Segment

Gains

Easily actionable

Specified alerts

Customer Job(s)

Respond to alerts

Assess risk of users

Validate user access

Pains

What's abnormal?

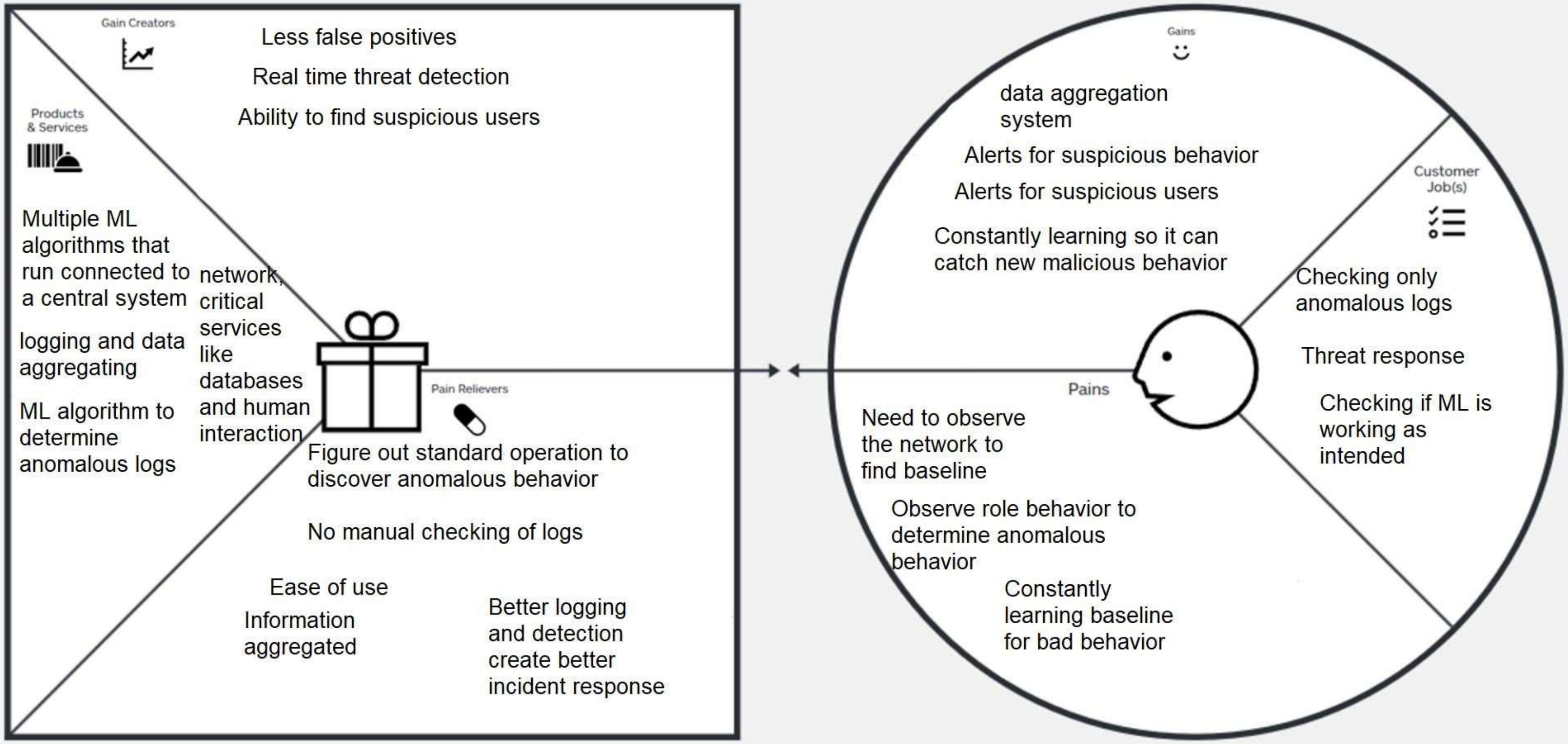
Defining a baseline for behavior

Dani Saba

The Value Proposition Canvas

Value Proposition

Customer Segment



Gain Creators

Less false positives

Real time threat detection

Ability to find suspicious users

Products & Services

Multiple ML algorithms that run connected to a central system

logging and data aggregating

ML algorithm to determine anomalous logs

network, critical services like databases and human interaction

Pain Relievers

Figure out standard operation to discover anomalous behavior

No manual checking of logs

Ease of use

Information aggregated

Better logging and detection create better incident response

Gains

data aggregation system

Alerts for suspicious behavior

Alerts for suspicious users

Constantly learning so it can catch new malicious behavior

Customer Job(s)

Checking only anomalous logs

Threat response

Checking if ML is working as intended

Pains

Need to observe the network to find baseline

Observe role behavior to determine anomalous behavior

Constantly learning baseline for bad behavior

Interview Slide

- [redacted] - Lecturer in RIT CSEC Department
- [redacted] - Lead CIRT Cloud Analyst
- [redacted]RT Cloud Lead
- [redacted] Security Engineer
- [redacted] - Computer Science student
- [redacted] - Amtrak Security Engineer
- [redacted] CSEC Student
- [redacted] CSEC Masters Student
- [redacted] - CSEC Student
- [redacted] - Lecturer in RIT CSEC Department
- [redacted] - Red Team Intern at SRA
- [redacted] - Lecturer at RIT; Cyber Security Consultant
- [redacted]Ops Engineer
- [redacted] - Security Engineer