Building a Validator For SaaS Provider's Reason for Accessing Customer Data

Presented by Jack Cha

Product Security Engineer, CSSLP, GCCC, GLEG, GCIA, GCIH, GSEC, GWAPT, GPEN

Master's Degree Candidate at the SANS Technology Institute

Presented to fulfill degree requirements for the SANS Technology Institute's Master of Science

Whitepaper Link – SANS Reading Room

Objectives

- Understand a typical SaaS company’s need for interacting with customer data and where the records are
- Understand how your security team can build a monitor function to validate customer data access events
  - Start shifting from Role Based to Need Based
- Question: Does your organization have a similar capability?

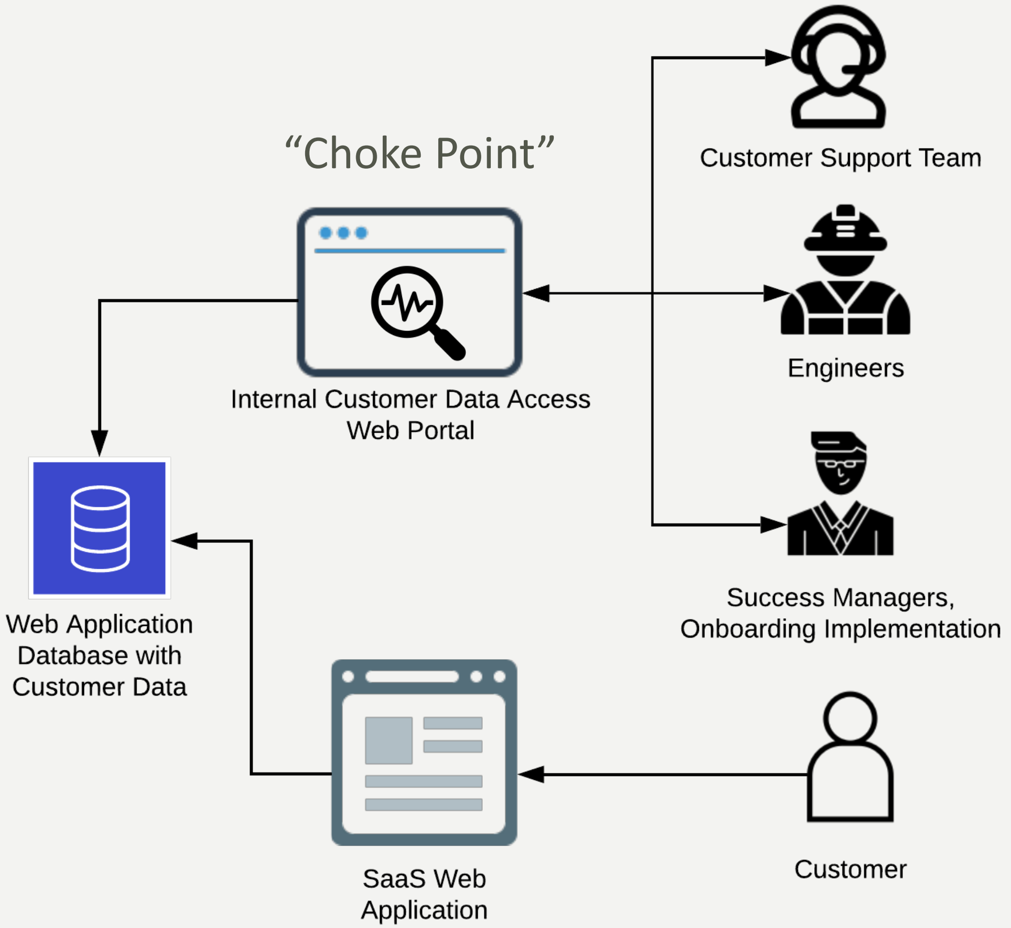
Why?

- CCPA / GDPR calls for modern privacy capabilities:
  - Data deletion, Data portability
  - Prompting companies to develop advanced privacy programs
- Perfect opportunity for your security team
  - Get closer to the business and its people
  - To understand access patterns, you have to gain insights to business functions
  - Change the culture
- Reduce exposure to customer data – make teams conscious

SaaS Company and its Workers

- Great services comes with data access
    - Customer Support
    - Implementation
    - Customer Advisors / Success Managers
    - Engineering
- As business grows, workforce grows with complex access patterns
- First challenge: Find the perfect choke point to capture customer data access events

Customer Data Access Web Portal



“Choke Point”

Internal Customer Data Access Web Portal

Customer Support Team

Engineers

Success Managers, Onboarding Implementation

Web Application Database with Customer Data

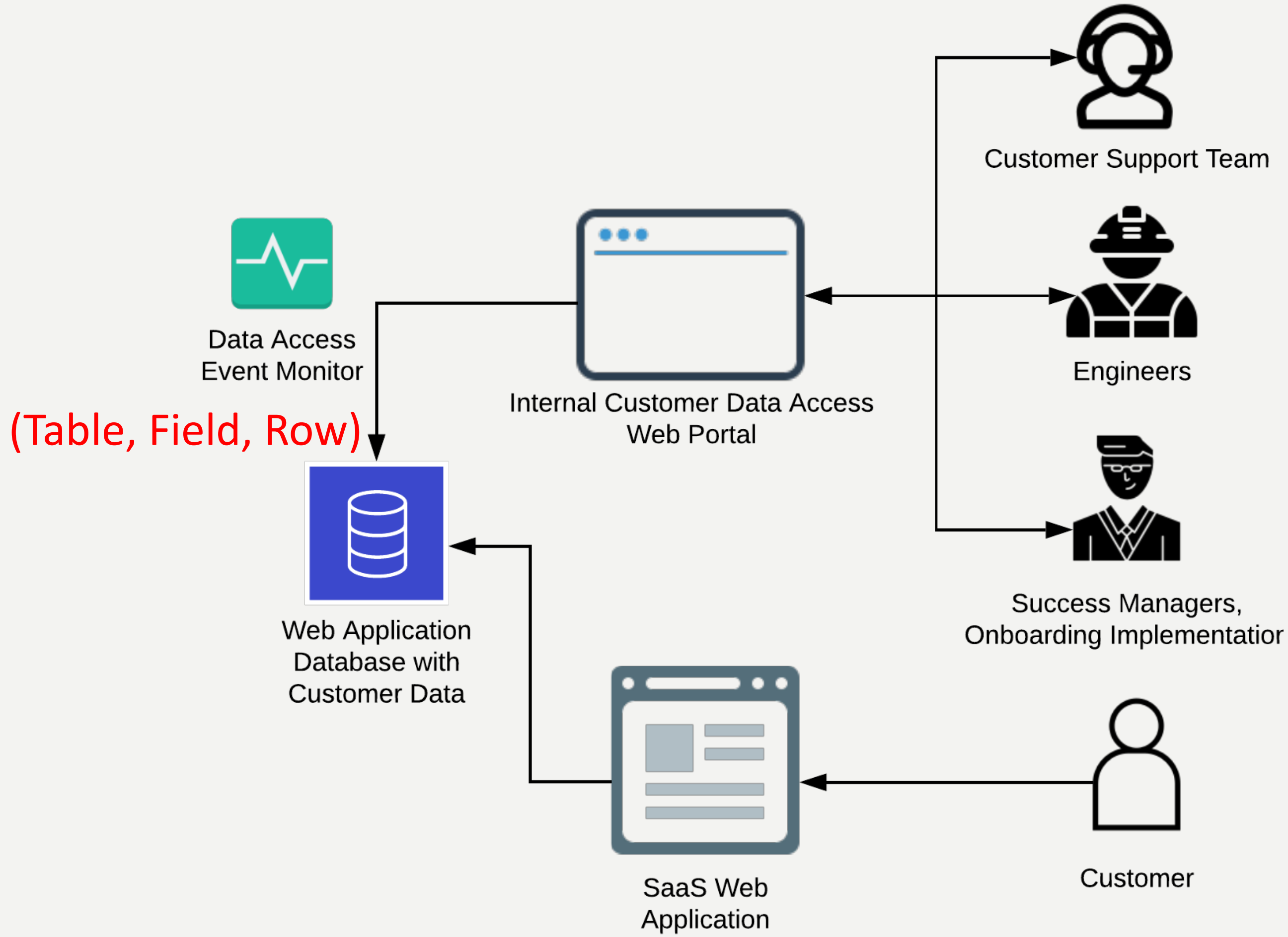
SaaS Web Application

Customer

First Step is to Record

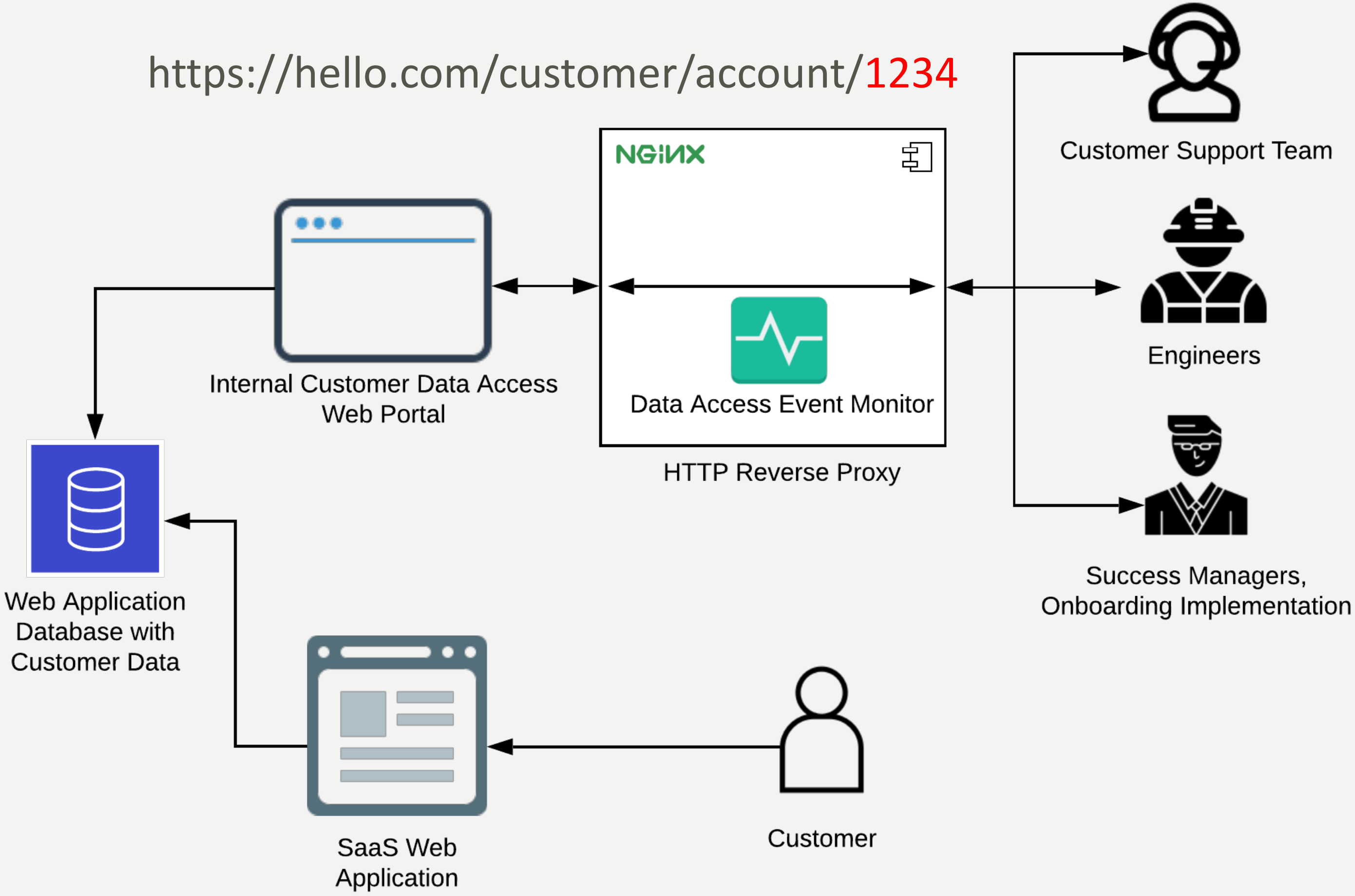
- Need to Record:
  - Who accessed the customer data
  - Which customer’s data was accessed
  - When was customer data access
- Where would be the best way to build a monitor function?
  - Let’s explore few options and talk about cost & complexity

Building a Monitor Function – Option 1



Building a Monitor Function – Option 2

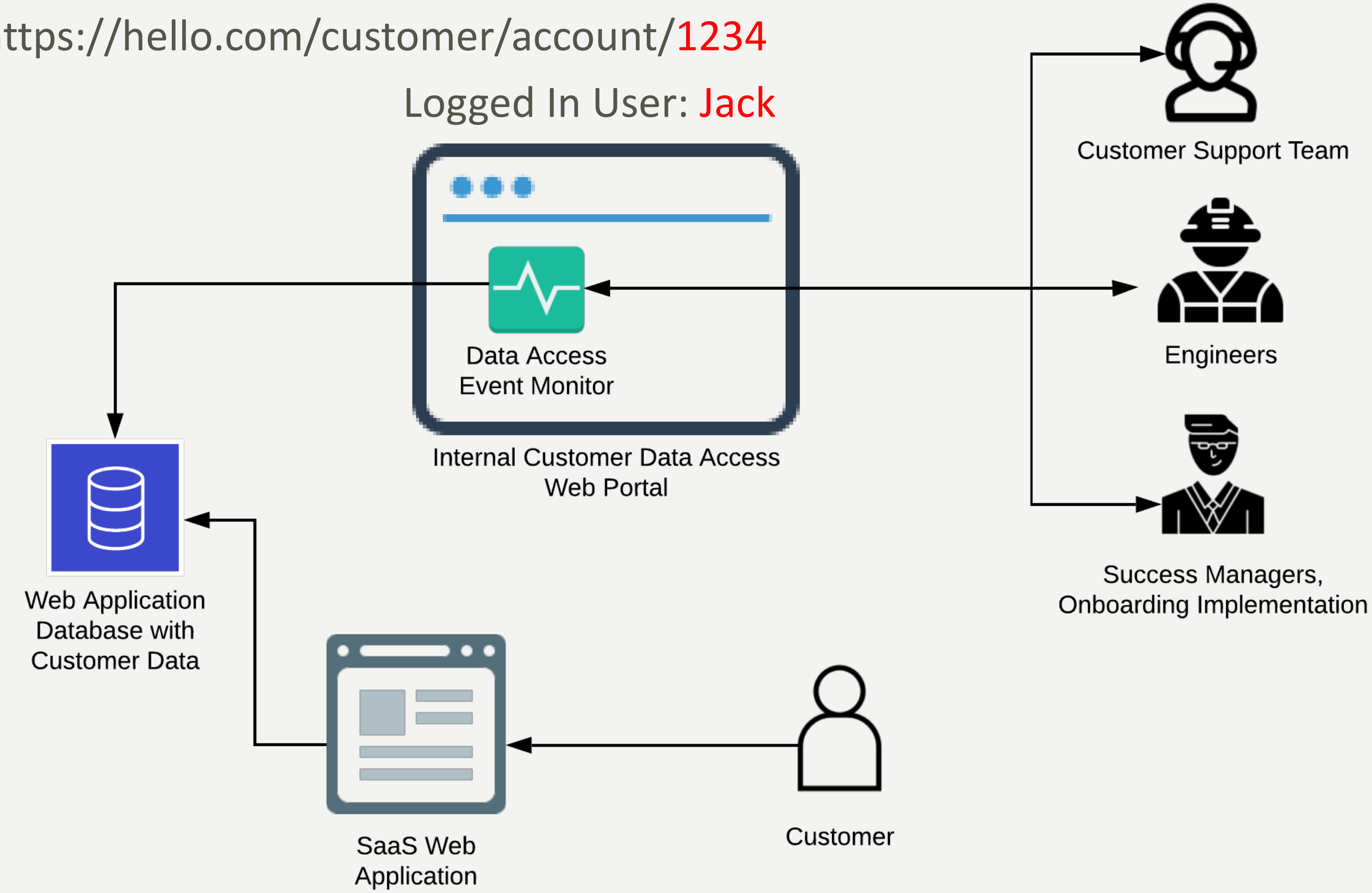
https://hello.com/customer/account/1234


NGINX
Customer Support Team
Internal Customer Data Access Web Portal
Data Access Event Monitor
Engineers
HTTP Reverse Proxy
Web Application Database with Customer Data
Success Managers, Onboarding Implementation
SaaS Web Application
Customer

Building a Monitor Function – Option 3

https://hello.com/customer/account/1234

Logged In User: Jack


Customer Support Team
Engineers
Success Managers, Onboarding Implementation
Data Access Event Monitor
Internal Customer Data Access Web Portal
Web Application Database with Customer Data
SaaS Web Application
Customer

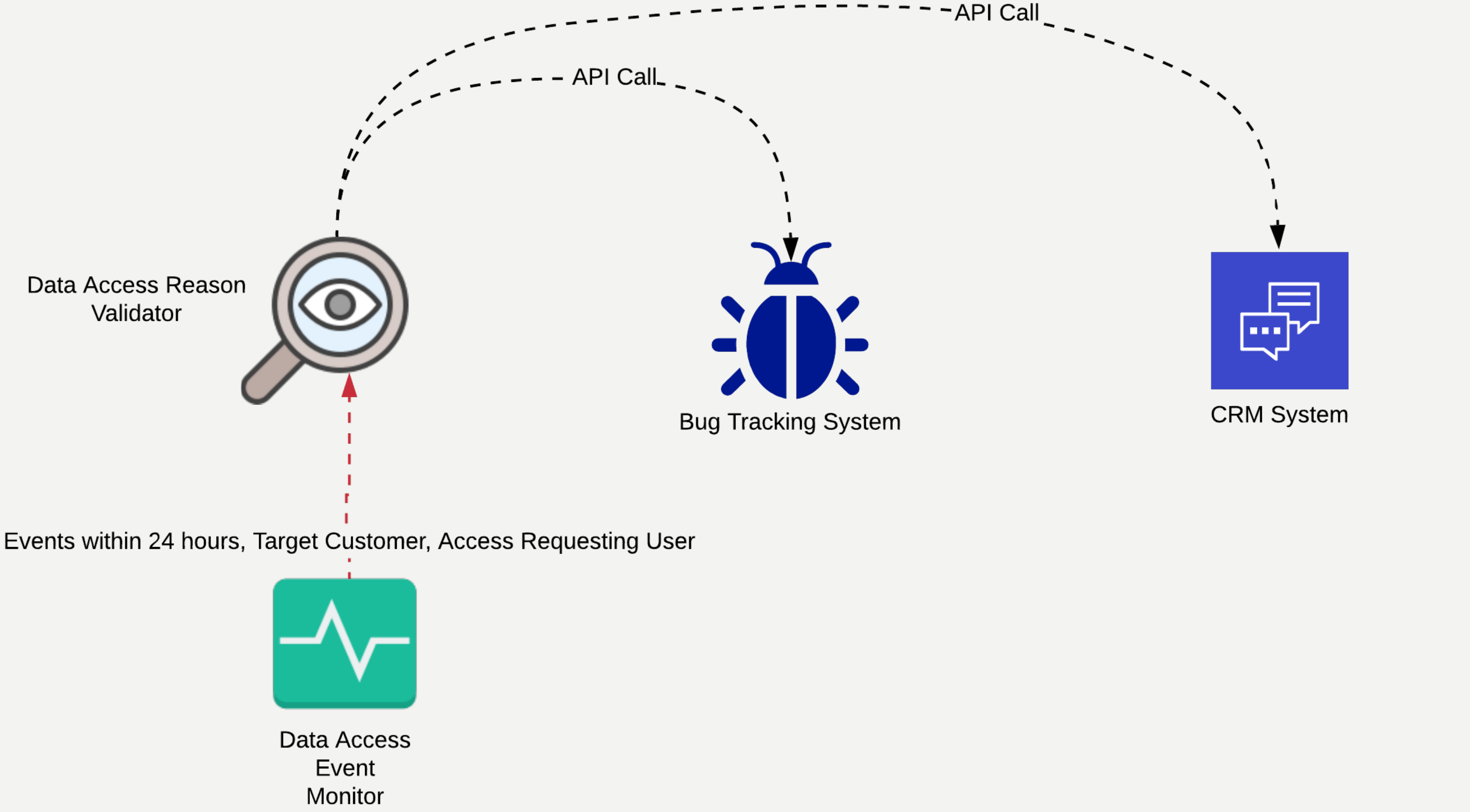
Second Step is to Validate

- Finding a record that can prove the need
    - CRM – Customer Cases
    - Bug Tickets involving a customer account
    - Internal work task items
        - Onboarding, Implementation
- Like a treasure hunt
    - Series of interviews with each teams
    - Find objects and fields that has linkage to Customer ID

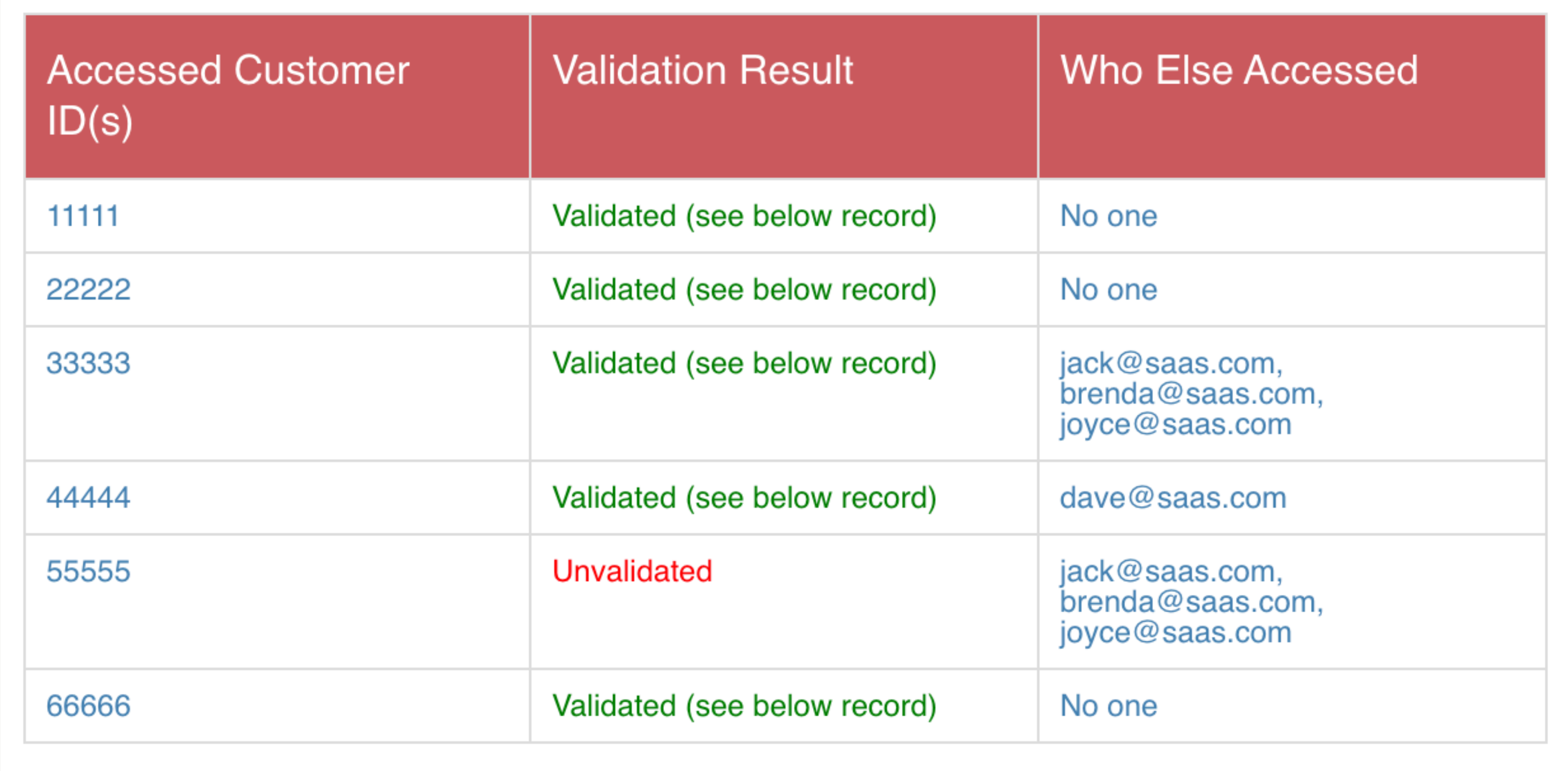
Uncovering Workflows

- Conduct initial discovery interviews with each team
- Conduct in-depth interviews with validation trials
- Tips:
  - Purpose is not to suggest a strict "one size fits all" workflow to all teams
  - Listen, learn, and be humble
  - Be sure to let them know it is not an audit of any kind
  - But let it be known that such monitoring capability is there!

Building a Validator Function

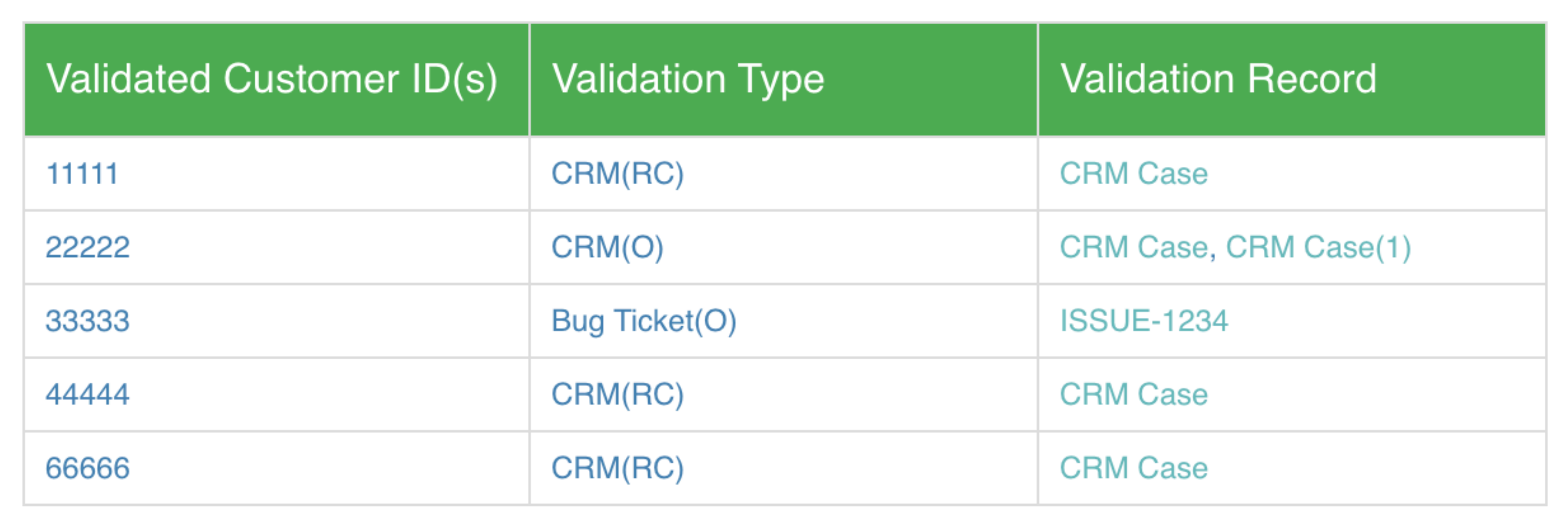

API Call
API Call
Data Access Reason Validator
Bug Tracking System
CRM System
Events within 24 hours, Target Customer, Access Requesting User
Data Access Event Monitor

Sample Validation Run



Accessed Customer ID(s)	Validation Result	Who Else Accessed
11111	Validated (see below record)	No one
22222	Validated (see below record)	No one
33333	Validated (see below record)	jack@saas.com, brenda@saas.com, joyce@saas.com
44444	Validated (see below record)	dave@saas.com
55555	Unvalidated	jack@saas.com, brenda@saas.com, joyce@saas.com
66666	Validated (see below record)	No one

Sample Validation Records Found

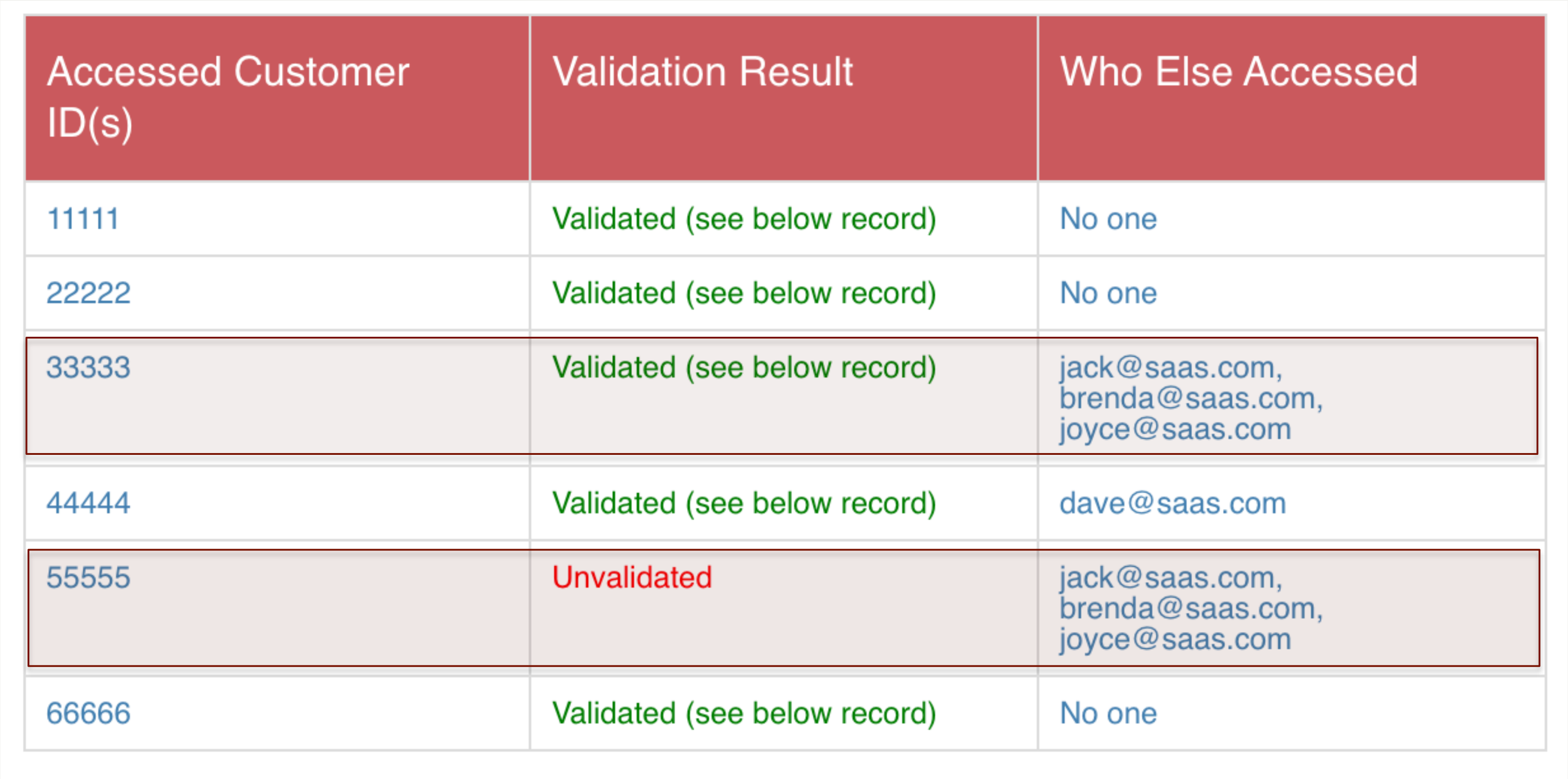


Validated Customer ID(s)	Validation Type	Validation Record
11111	CRM(RC)	CRM Case
22222	CRM(O)	CRM Case, CRM Case(1)
33333	Bug Ticket(O)	ISSUE-1234
44444	CRM(RC)	CRM Case
66666	CRM(RC)	CRM Case

Captured Workflow in CRM/Bug Tracker

Department	Access Volume	CRM	Bug Tracker	Test Account	Captured Workflow
Customer Support	High	81%	0%	14%	95%
Customer Advisor	Medium	90	5%	0%	95%
Engineering	Low	75	8%	0%	83%
Other	Low	38	19%	8%	57%
Implementation	Highest	5%	40%	11%	56%

Team Work Patterns



Accessed Customer ID(s)	Validation Result	Who Else Accessed
11111	Validated (see below record)	No one
22222	Validated (see below record)	No one
33333	Validated (see below record)	jack@saas.com, brenda@saas.com, joyce@saas.com
44444	Validated (see below record)	dave@saas.com
55555	Unvalidated	jack@saas.com, brenda@saas.com, joyce@saas.com
66666	Validated (see below record)	No one

Uncaptured Workflows

- Customers with similar past issues
- Solving an underlying issue that affects multiple customers who hasn’t filed a ticket yet
- Book of Business
- Contract renewal period
- Onboarding / Offboarding

Just as a Starting Point

- CRM and Bug Tracking System did not contain all workflows
- But, created a rational data backed discussion point to discover each team’s workflows
- Excellent opportunity to gain holistic insight into all business operations
- Future Research
    - Access Behavior Analytics Engine
    - Active Gating Mode

Questions? Ideas?

- Jack Cha
    - LinkedIn
    - jackcha83@gmail.com