Payment Card Fraud

How SecurePay Mitigates Card Washing Attacks

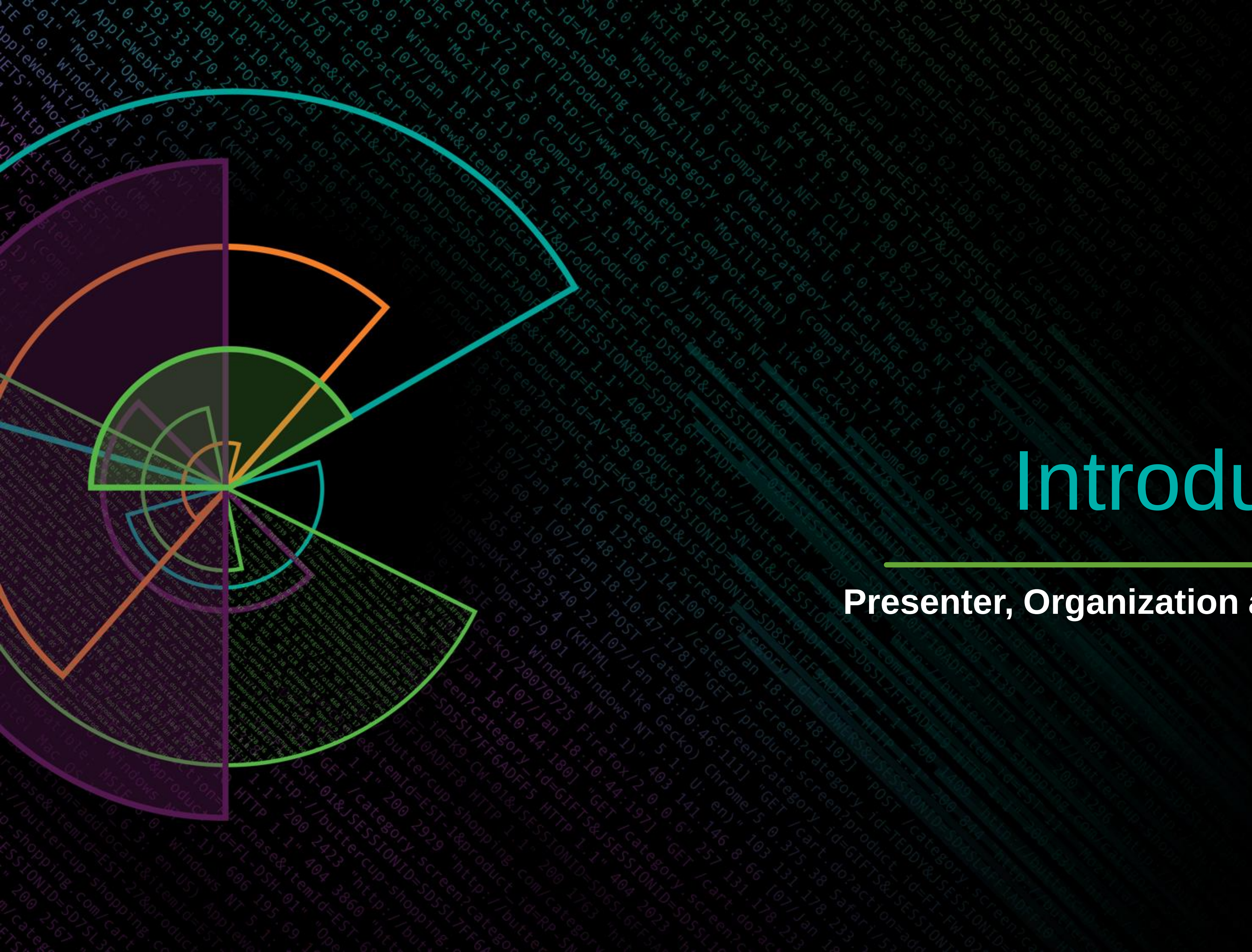
Presented By: Luke Bampton

October 2018

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.



Introductions

Presenter, Organization and Definition

LUKE BAMPTON

Application Security Specialist
SecurePay (Australia Post)

About SecurePay

Powering online payments for Australian business

- Established in 1999 to facilitate online eCommerce credit card transactions
- Provides payment solutions to all types of businesses from Enterprise and Government to Micro and SMB
- Acquired by Australia Post in 2010

SecurePay facilitates AUD$50 - $60M in transactions every day.

- One of the largest providers of online transaction processing in Australia
- Fully Payment Card Industry Data Security Standard (PCI DSS) v3.2 Compliant as a Level 1 service provider
- Certified compliant to ISO:270001:2013

SecurePay

Card Washing is the act of validating a list of credit cards in bulk for later use

What is Card Washing?

And who are we up against?

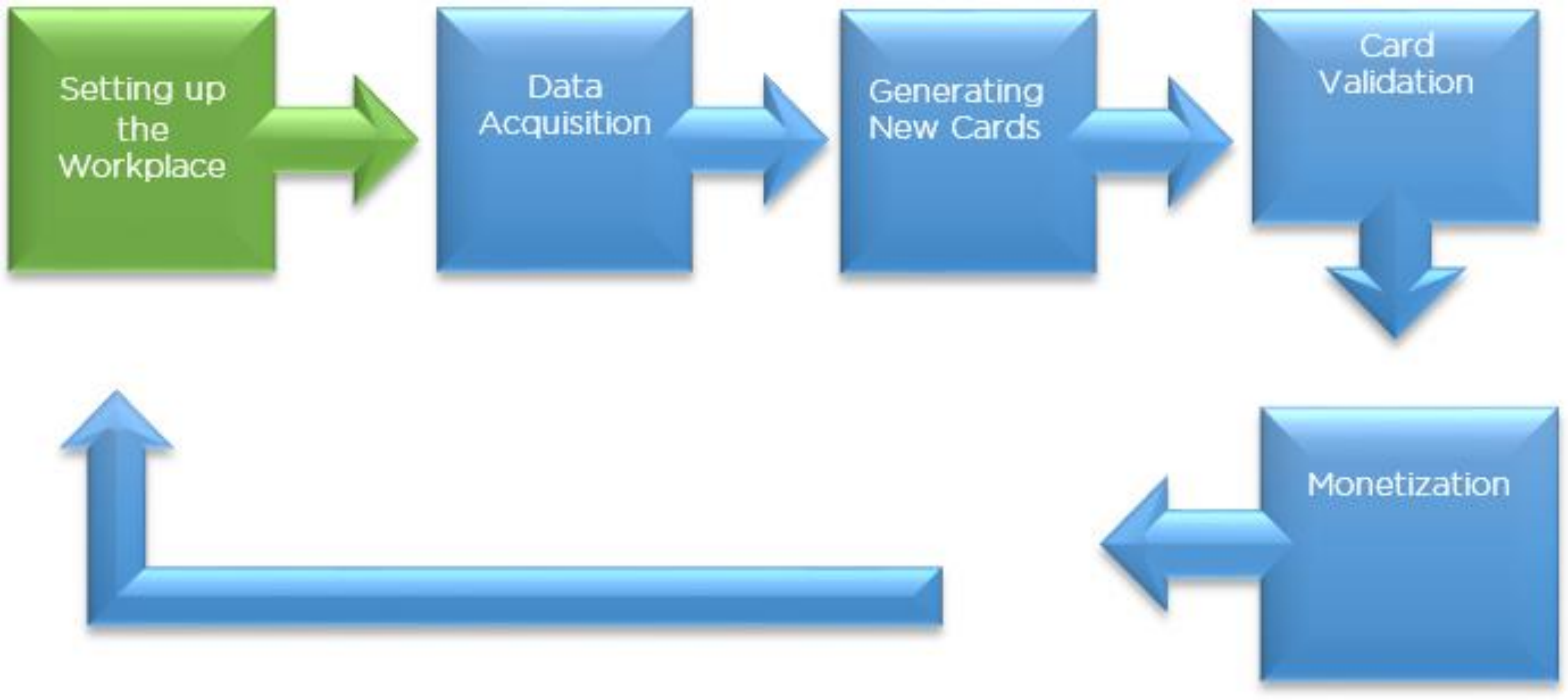
- Cybercriminals who specialize in payment card fraud either buy or obtain large data sets of credit card data and then attempt to verify the validity of that stolen data using differing techniques with the aim of selling on validated cards at a premium or to use them for fraud in order to monetize.

- These Cybercriminals use a variety of different methods to either compromise or acquire already compromised payment card credentials, including sharing or purchasing dumps online, hacking vulnerable merchant websites and compromising payment card processing devices. The compromised payment card credentials can also be used to generate further card information. The main methods used to launder and monetize illicit funds include online purchases of various goods and services as well as ATM withdrawals.

- It is amazing the extent to which Cybercriminal organisations display characteristics of a sophisticated business operations taking advantage of technology including the scalability and power of cloud computing and the use of automation to create tools to identify vulnerable payment interfaces and perform card washing activities as well as evade detective and preventative anti fraud controls. Such actors use tools commonly known as "card generators" to generate new card numbers based on the compromised ones, creating additional opportunities for monetization.

How the process works

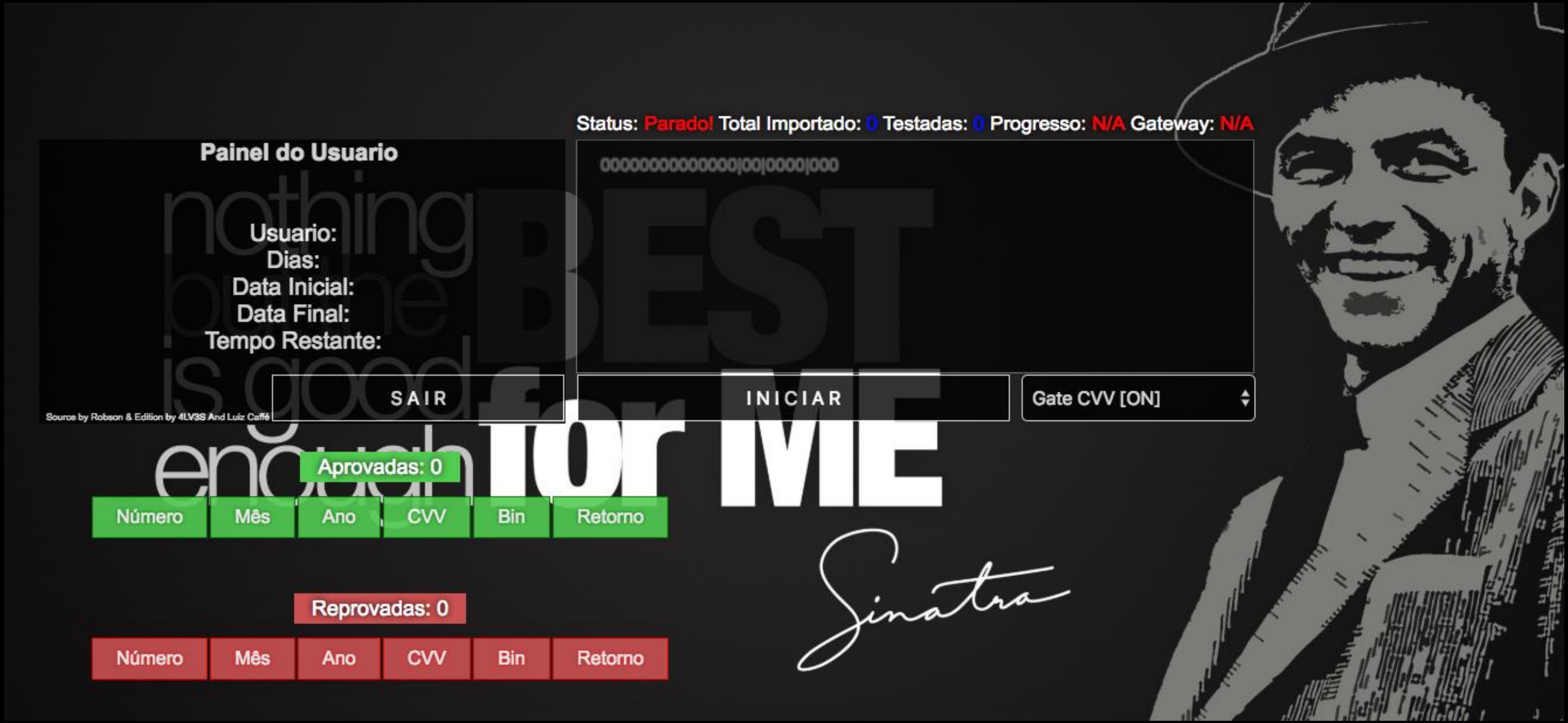
Operational processes of payment fraud cybercrime organizations



- Reference: https://www.fireeye.com/blog/threat-research/2016/10/operations_of_a_braz1.html

Card Washing Tool

Using card washing tools to attempt to compromise a system



Status: Parado! Total Importado: 0 Testadas: 0 Progresso: N/A Gateway: N/A

00000000000000|00|0000|000

Painel do Usuario

Usuario:
Dias:
Data Inicial:
Data Final:
Tempo Restante:

Source by Robson & Edition by 4LV3S And Luiz Caffé

Gate CVV [ON]

Aprovadas: 0

Número	Mês	Ano	CVV	Bin	Retorno

Reprovadas: 0

Número	Mês	Ano	CVV	Bin	Retorno

Problem Scope

How much of a problem is Card Washing?

Card washing is a significant problem

Findings from AusPayNet Australia Payment Card Fraud Report 2018

- According to the Australian Payment Card Fraud 2018 report released by AusPayNet, Australia’s self-regulatory body and industry association for payments:
  - Card fraud [in Australia] of all types was up 5% to $561 million and accounted for 0.075% of the overall value of card transactions. As the overall value of transactions was also up 5% to $748.1 billion, the rate of card fraud remained largely the same as in 2016.
  - As in-person fraud becomes harder, and as more payments are made online, fraud is migrating to card-not-present channels. Almost 85% of card fraud now occurs online, reflecting a global trend of growing online card fraud and cybercrime generally.
  - In 2017, online fraud totalled $476.3 million, representing 87.5percent of all fraud on scheme cards. This compares to 75 percent in 2012

    - Reference: https://www.auspaynet.com.au/sites/default/files/2018-08/AustralianPaymentCardFraud-2018-Report.pdf

> “Almost 85% of card fraud now occurs online, reflecting a global trend of growing online card fraud…”

AusPayNet - Australian Payment Card Fraud 2018

What is the impact?

Who is paying the bill?

- Fraudulent payments directly cost merchants in the form of chargebacks and payment gateways in the form of refunded transaction fees as well the indirect costs of the time and effort to manage these processes. Given enough volume, the card schemes (Visa/Mastercard) can get directly involved.

- Cardwashing can occur against any unauthenticated payment interfaces, which commonly exist to allow frictionless payments like donations to charities and other non-profits who need the process to be as easy as possible. Merchant transaction accounts can also be compromised through poor security practices i.e easily guessable passwords and cardwashing activities then occur.

- Overall, fraudulent activity has the potential to damage trust in card schemes and for specific companies and is not a victimless crime. The costs to manage fraud are borne through higher transaction/processing fees.

Detect > Analyse > Respond > Monitor

How SecurePay addresses Card Washing

Existing Problems

In summary, the previous process was:

- Not scalable
- Development work required
- Too slow
- Manual actions required
- Lack of alerting

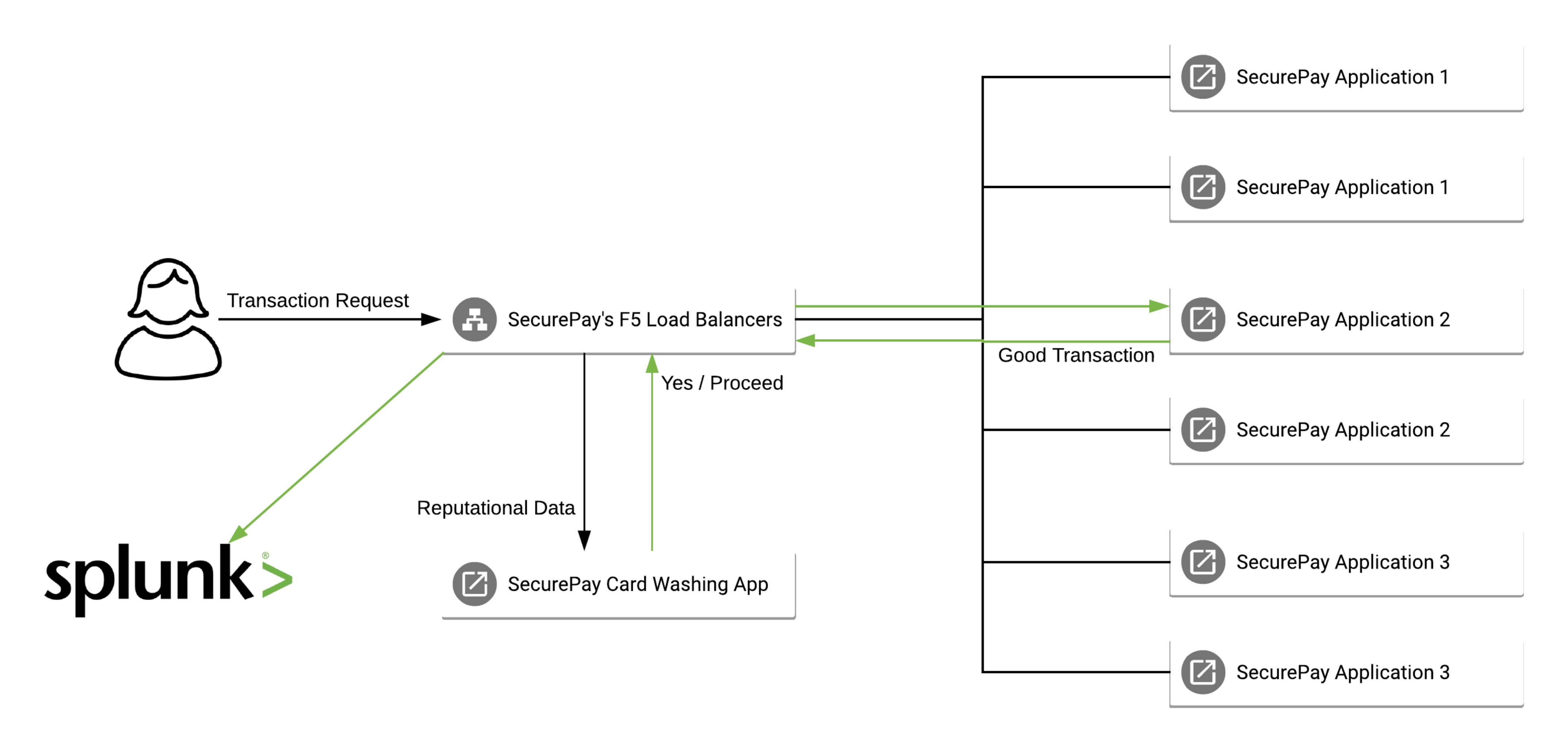
SecurePay’s Solution

What we built to solve those problems

- Identified an opportunity to extend our Web Application Firewall to enforce differing rule sets for differing interfaces
- Categorised and prioritised the payment interfaces and platforms
- Important that B2B interfaces saw as little impact as possible
- Most of the Card Washing activity occurred on non-authenticated C2B channels
- Blocking would be IP address based and only be enforced for a set duration
- IP Address blocks would be automatically enforced and automatically lifted
- Able to manually lift a block in the event of an incident
- Able to whitelist customer IP addresses by mutual agreement
- Leverages Splunk for Event logging, analysis, alerting and reporting

A Valid Request

A normal transaction



Transaction Request

SecurePay's F5 Load Balancers

Reputational Data

Yes / Proceed

SecurePay Card Washing App

Good Transaction

SecurePay Application 1

SecurePay Application 1

SecurePay Application 2

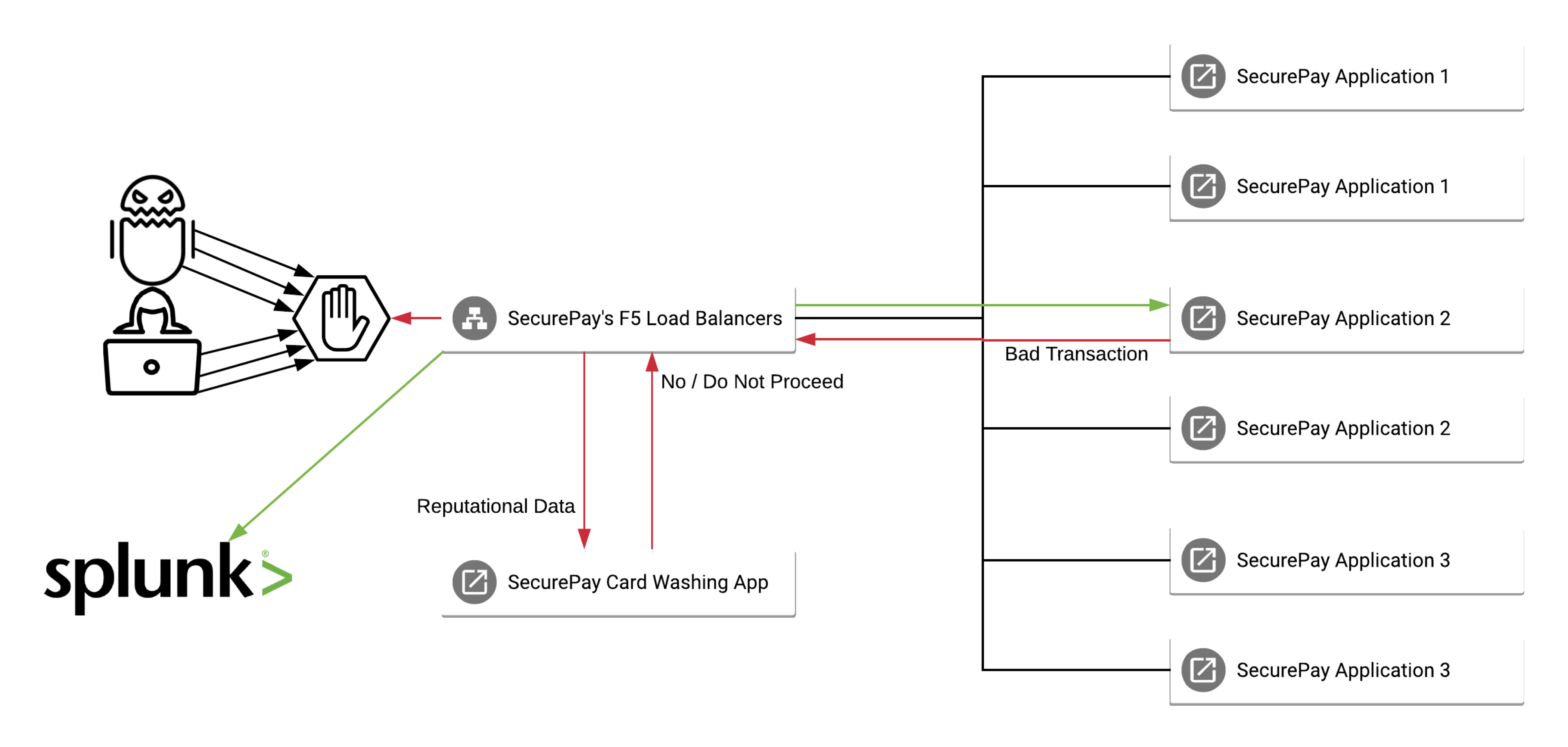
SecurePay Application 2

SecurePay Application 3

SecurePay Application 3

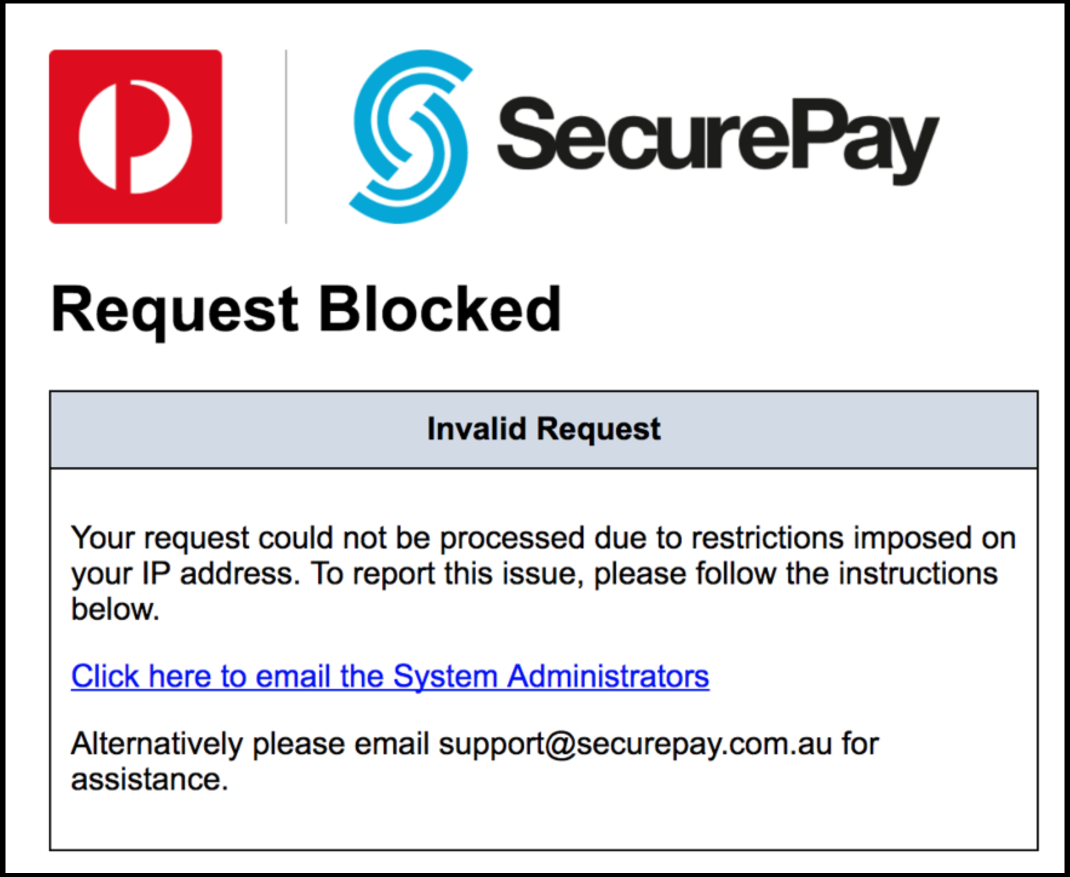
An Invalid Request

Card washing requests



The Result

The resulting Block Page served instead of processing the payment



SecurePay

Request Blocked

Invalid Request
Your request could not be processed due to restrictions imposed on your IP address. To report this issue, please follow the instructions below. Click here to email the System Administrators Alternatively please email support@securepay.com.au for assistance.

The Awesome Features

The best bits!

- No Development work required. Implemented and administered by Cyber Security
- Can be load balanced / scaled if required
- Does not replace proprietary fraud mitigation offerings
- Botnet ready. Attackers can’t simply change IP address
- Splunk logging & proactive alerting of all IP’s suspected of card washing
- Designed to support non-blocking / reporting mode
- 100% automated, no manual intervention required. Blocks are lifted automatically.
- Tuneable rules to react to new threats
- Self-cleaning local database

Solution Summary

In summary, the new process is:

Flexible

Fully Monitored

Fully Automated

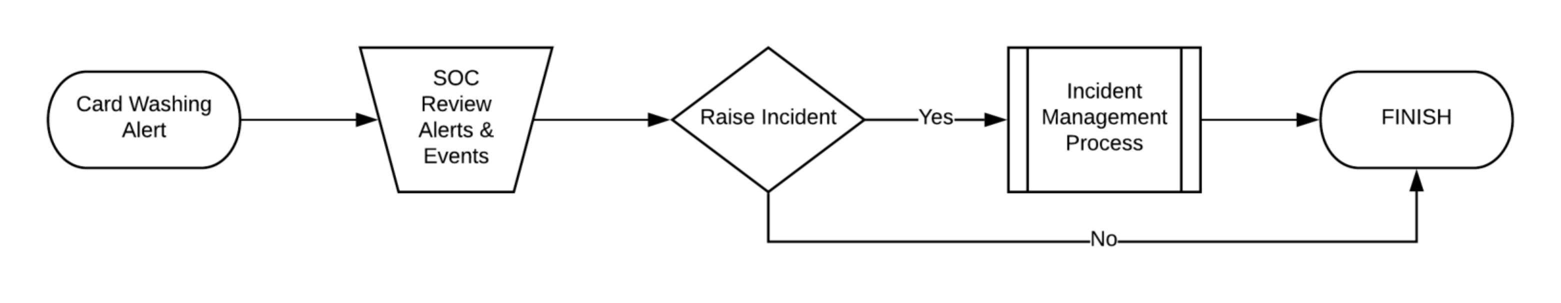
The “Secret Sauce”

How SecurePay leverages Splunk

Our Use of Splunk

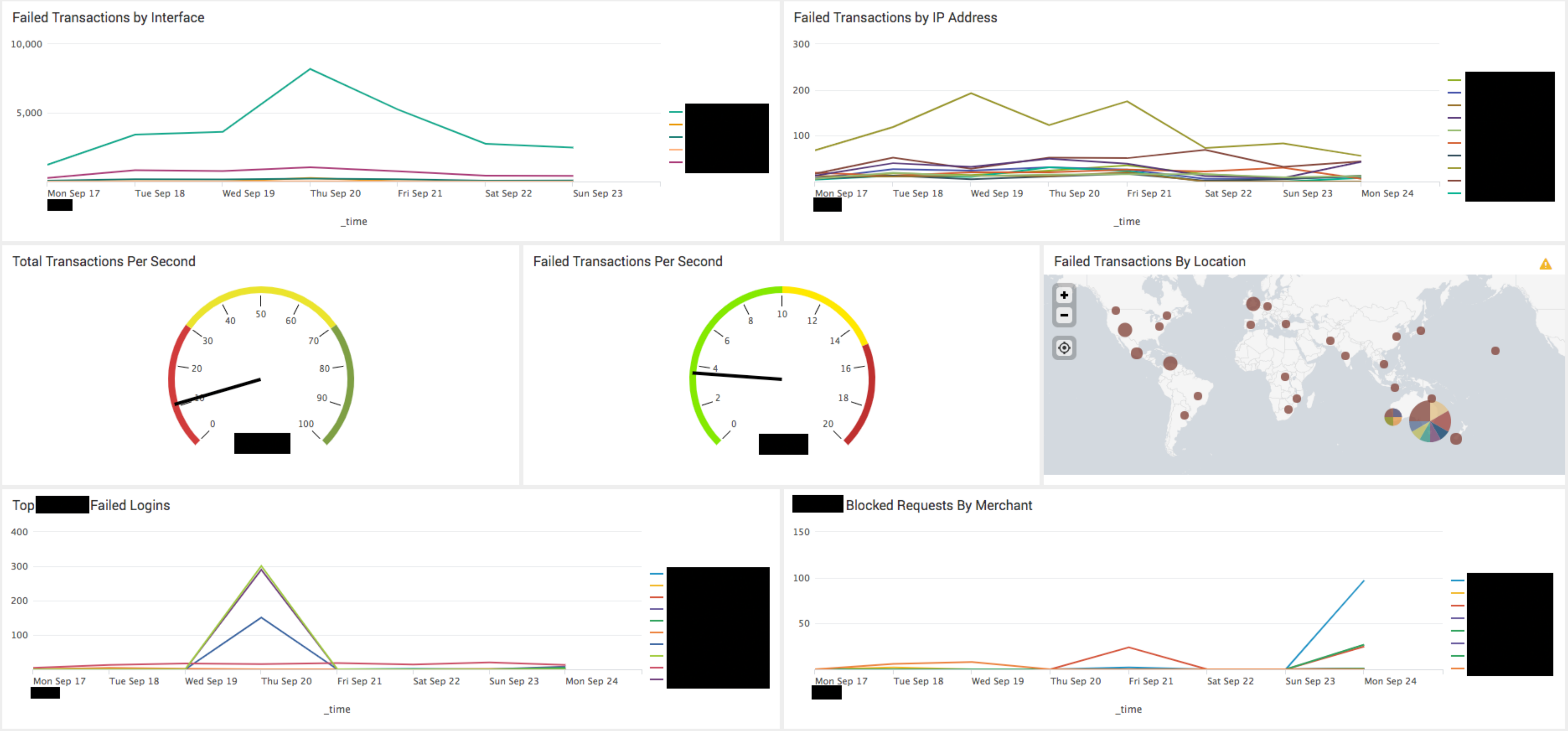
What you have all been waiting for

- Each transaction logs a data set specific to the payment interface
- Core Data Points:
  - Time
  - Transaction Result
  - Transaction Duration
  - Client IP Address
  - Payment Interface
  - Hostname
  - Merchant ID
  - Amount
  - Transaction Response Code
  - Transaction Reference
- Analysis made possible by this logging:
  - Platform Throughput
  - Approvals vs Declines
  - User behaviour analysis
  - IP Geolocation for market trends
  - Capacity planning for internal applications
  - High visibility of repeat offenders



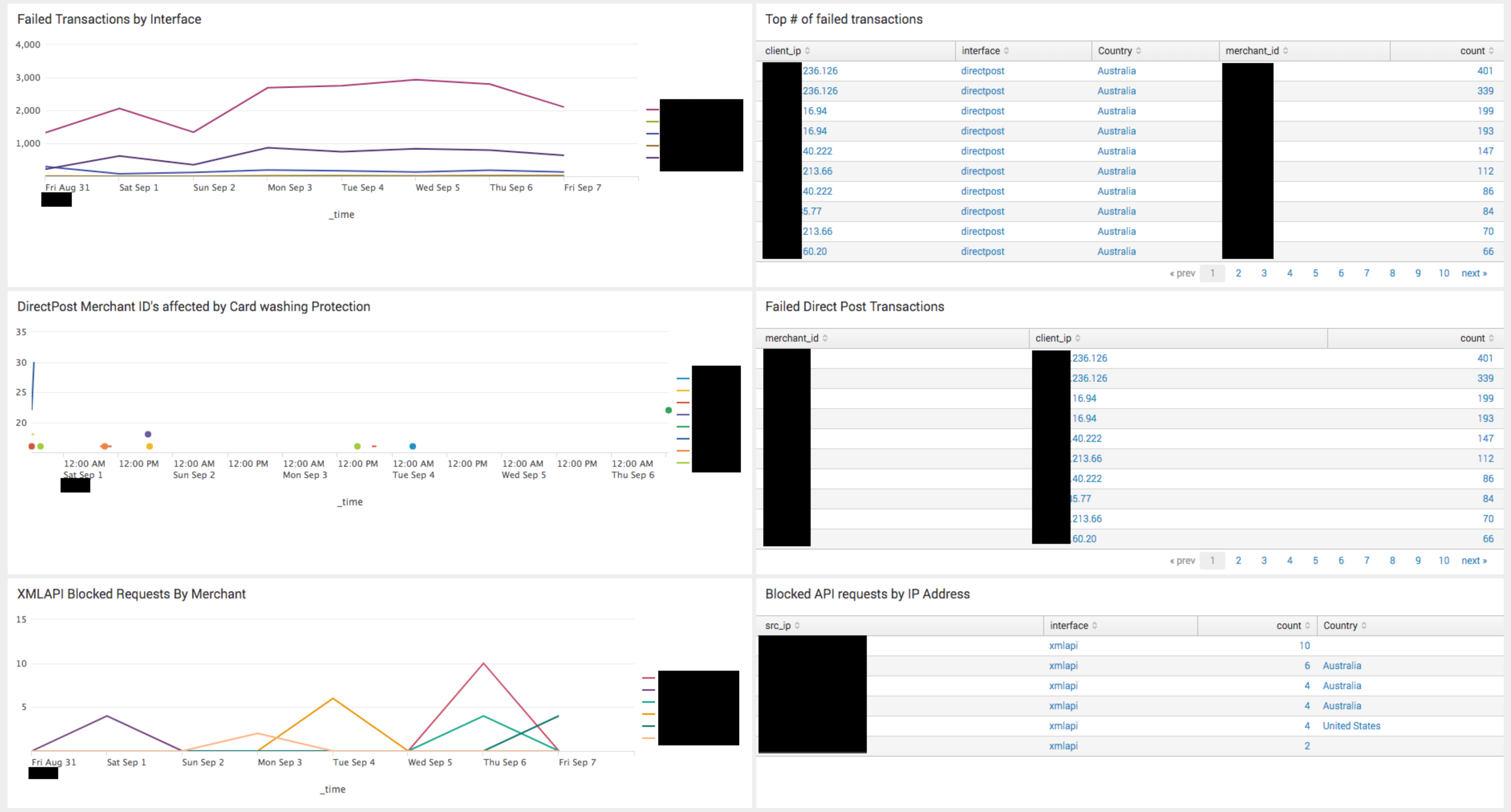
Our Use of Splunk

What you have all been waiting for



Our Use of Splunk

What you have all been waiting for



Failed Transactions by Interface

[redacted]

Top # of failed transactions

client_ip	interface	Country	merchant_id	count
[redacted]236.126	directpost	Australia	[redacted]	401
[redacted]236.126	directpost	Australia	[redacted]	339
[redacted]16.94	directpost	Australia	[redacted]	199
[redacted]16.94	directpost	Australia	[redacted]	193
[redacted]40.222	directpost	Australia	[redacted]	147
[redacted]213.66	directpost	Australia	[redacted]	112
[redacted]40.222	directpost	Australia	[redacted]	86
[redacted]5.77	directpost	Australia	[redacted]	84
[redacted]213.66	directpost	Australia	[redacted]	70
[redacted]60.20	directpost	Australia	[redacted]	66

« prev 1 2 3 4 5 6 7 8 9 10 next »

DirectPost Merchant ID's affected by Card washing Protection

[redacted]

Failed Direct Post Transactions

merchant_id	client_ip	count
[redacted]	[redacted]236.126	401
[redacted]	[redacted]236.126	339
[redacted]	[redacted]16.94	199
[redacted]	[redacted]16.94	193
[redacted]	[redacted]40.222	147
[redacted]	[redacted]213.66	112
[redacted]	[redacted]40.222	86
[redacted]	[redacted]5.77	84
[redacted]	[redacted]213.66	70
[redacted]	[redacted]60.20	66

« prev 1 2 3 4 5 6 7 8 9 10 next »

XMLAPI Blocked Requests By Merchant

[redacted]

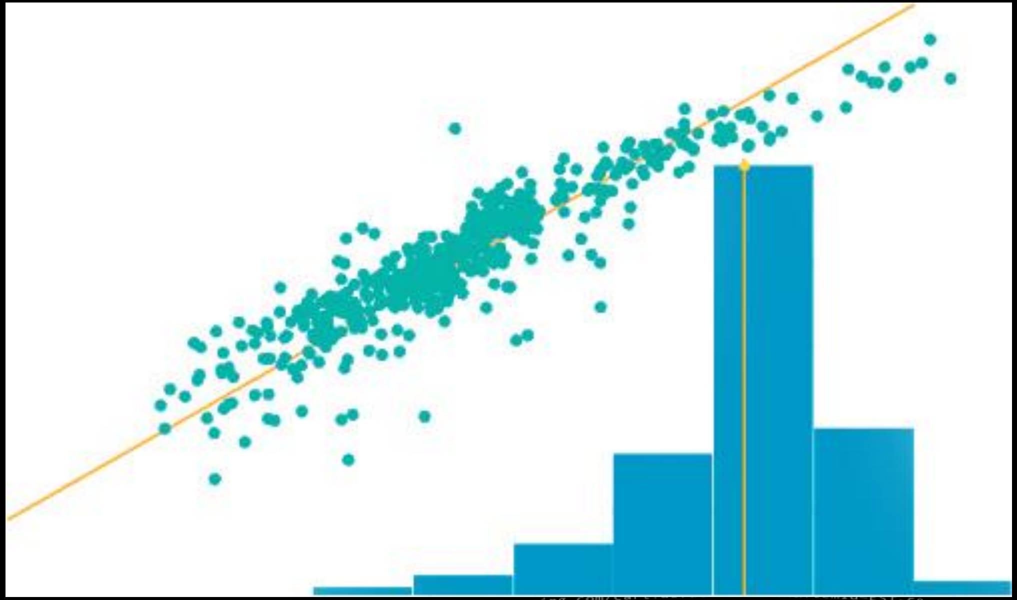
Blocked API requests by IP Address

src_ip	interface	count	Country
[redacted]	xmlapi	10	
[redacted]	xmlapi	6	Australia
[redacted]	xmlapi	4	Australia
[redacted]	xmlapi	4	Australia
[redacted]	xmlapi	4	United States
[redacted]	xmlapi	2	

Just the Beginning

What's Next?

- The Card Washing prevention tool has been a great success to date
- Future iterations will likely involve:
  - Splunk's Anomaly Detection– to identify baseline expected transaction volumes per merchant
    - These statistics can assist in raising alerts for accounts processing outlying volumes of transactions
  - Splunk's Predictive Analysis – to identify card washing incidents before they get a chance to ramp up in volume and impact to our customers.



Q&A

Luke Bampton | Application Security Specialist

Thank You

Don't forget to rate this session in the .conf18 mobile app

.conf18

splunk>

Fraud Analytics & Detection: .conf18 Presentations

- **SEC1400 - An Introduction to Fraud Detection With Splunk, Sony**
  - Tuesday, Oct 02, 3:30 p.m. - 4:15 p.m.
- **SEC1393 - Splunking for Fraud: Let the Machines Look for Unknown Unknowns**
  - Wednesday, Oct 03, 11:30 a.m. - 12:15 p.m.
- **SEC1601 - Payment Card Fraud – How SecurePay Mitigates Card Washing Attacks**
  - Wednesday, Oct 03, 3:15 p.m. - 4:00 p.m.
- **SEC1369 - Battling Against Online Bank Attacks/Attack Detection Methods Using Splunk**
  - Thursday, Oct 04, 11:00 a.m. - 11:45 a.m.
- **SEC1507 - Busting E-Commerce Scammers with Splunk, Intuit**
  - Thursday, Oct 04, 12:15 p.m. - 1:00 p.m.