# North America Community Meeting 2023

PCi Security Standards Council®

PCI Security Standards Council®

# Scaling 6.4.3 & 11.6.1: Browser Script Management & The Large Enterprise Journey to Compliance

# Introductions

## Steven Eric Fisher

Senior Cyber-Security Risk Expert,

Compliance

Walmart Global Tech*

## Jeff Zitomer

Sr. Director of Product Management,

Client-Side Defense & PCI DSS

HUMAN Security

** My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.*

PCI Security Standards Council ®

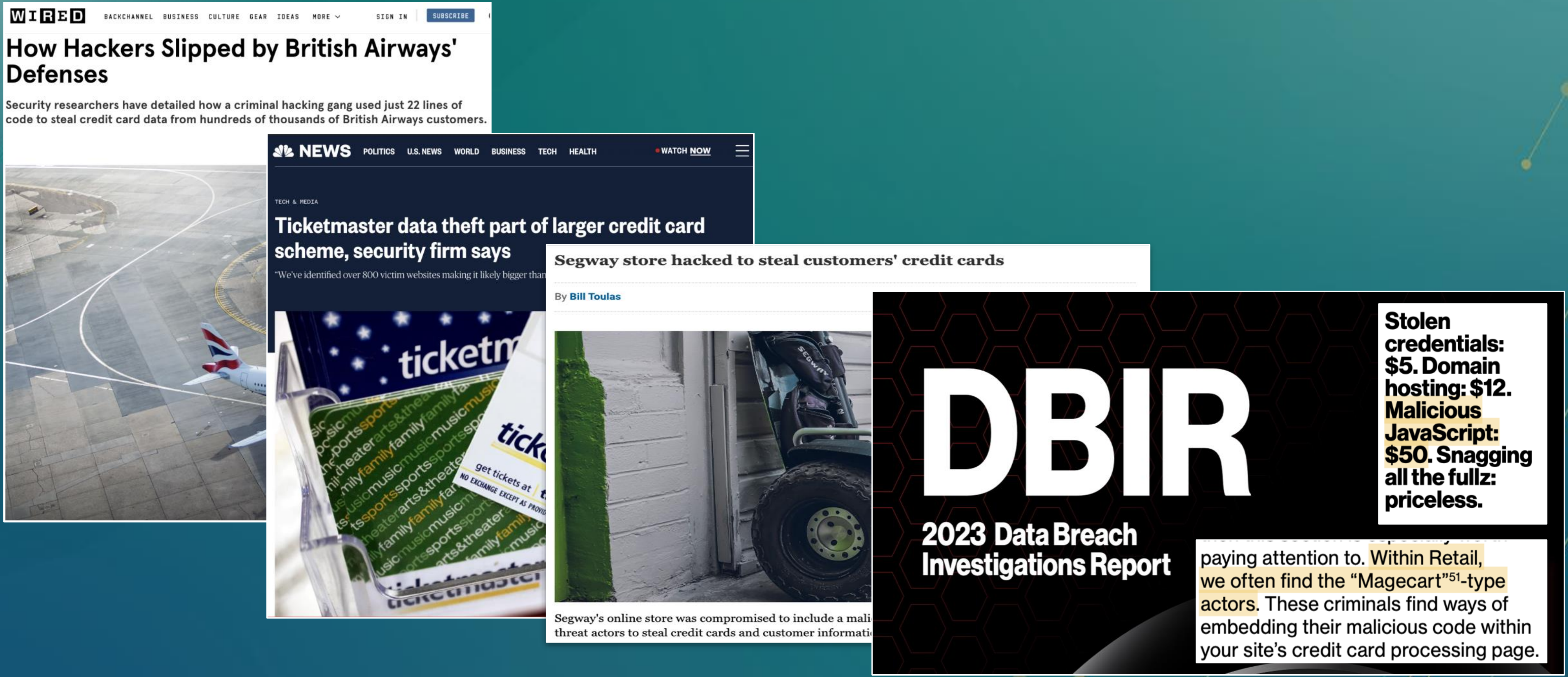
# Agenda

1. From Browser Script Risks to PCI DSS v4.0
2. The Large Enterprise Journey

# From Browser Script Risks to PCI DSS v4.0

Jeff Zitomer, HUMAN Security

# Script-Based Attacks “Became a Thing” Around 2018



**How Hackers Slipped by British Airways' Defenses**

Security researchers have detailed how a criminal hacking gang used just 22 lines of code to steal credit card data from hundreds of thousands of British Airways customers.

**Ticketmaster data theft part of larger credit card scheme, security firm says**

“We've identified over 800 victim websites making it likely bigger than

**Segway store hacked to steal customers' credit cards**

By Bill Toulas

Segway's online store was compromised to include a mali
threat actors to steal credit cards and customer informati

**DBIR**

**2023 Data Breach Investigations Report**

**Stolen credentials: $5. Domain hosting: $12. Malicious JavaScript: $50. Snagging all the fullz: priceless.**

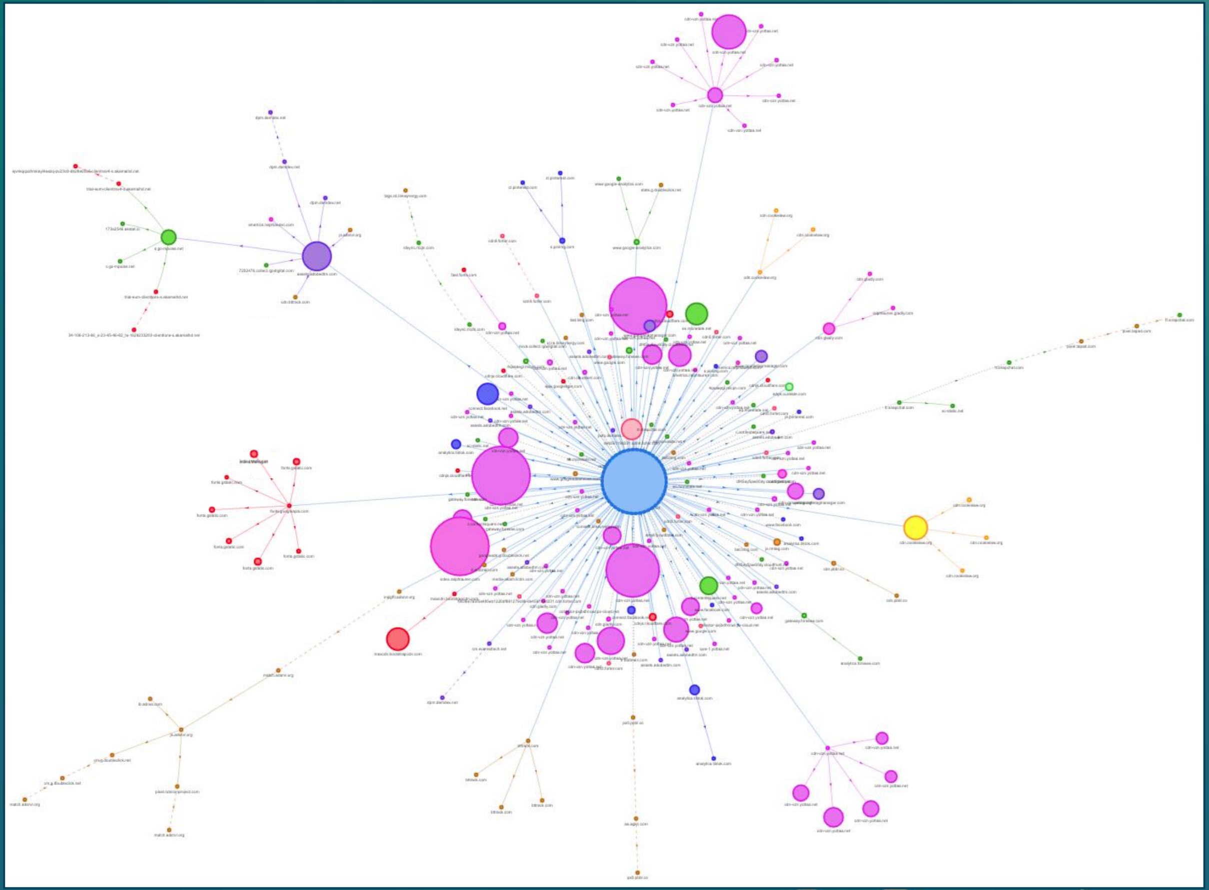
paying attention to. Within Retail, we often find the “Magecart”[51]-type actors. These criminals find ways of embedding their malicious code within your site’s credit card processing page.

PCI Security Standards Council ®

# Browser Scripts Are a Lucrative Attack Surface

## 1. Modern websites (and payment pages) heavily depend on them

- Analytics
- Promotion
- Advertising
- Social Media
- Chat & Support



# Browser Scripts Are a Lucrative Attack Surface

2. They load dynamically from across the Internet…

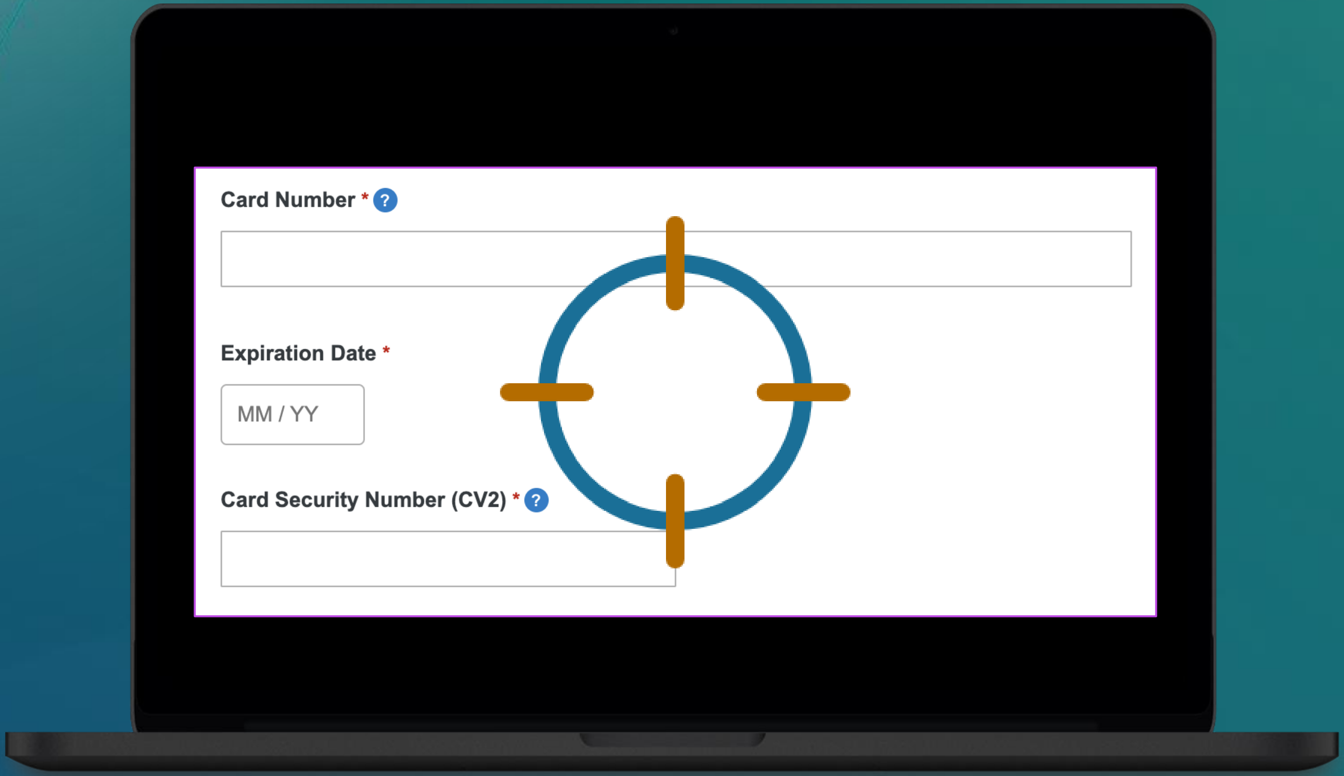
MOMMA ALWAYS SAID,
SCRIPTS WERE
~~LIFE WAS~~ LIKE A BOX OF CHOCOLATES.
YOU NEVER KNOW WHAT YOU'RE GONNA GET.
imgflip.com

# Browser Scripts Are a Lucrative Attack Surface

3. …bypassing change management & security controls

# Browser Scripts Are a Lucrative Attack Surface

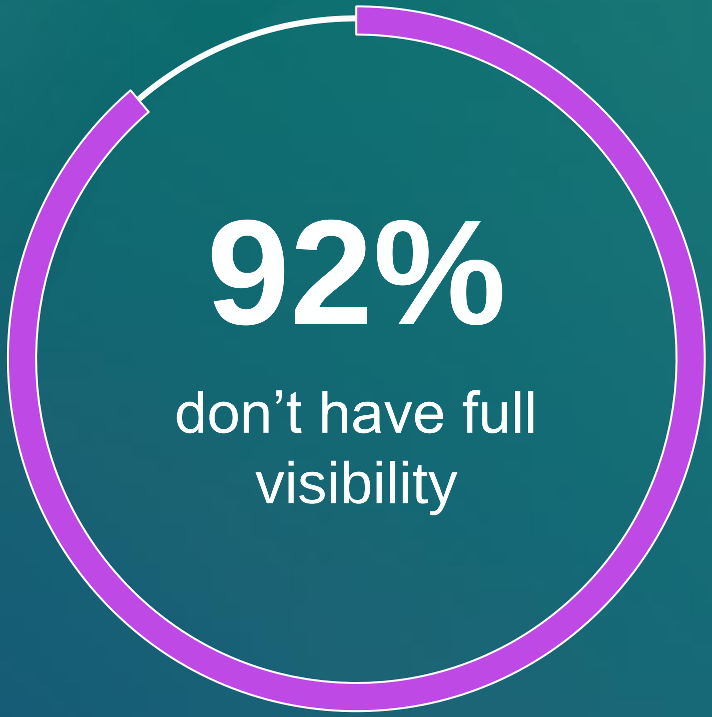
## 4. They can compromise cardholder data



- Skimming
- Formjacking
- Malicious Redirects

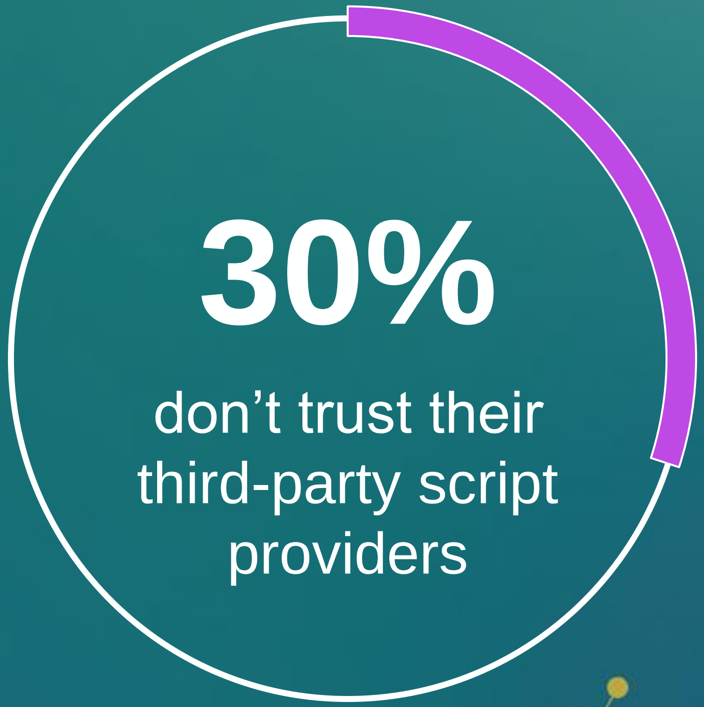
# Browser Scripts Are a Lucrative Attack Surface

## 5. They are largely unmanaged



**92%**

don’t have full visibility



**30%**

don’t trust their third-party script providers

Shadow Code: The Hidden Risk to Your Website, Survey by Osterman Report, 2020

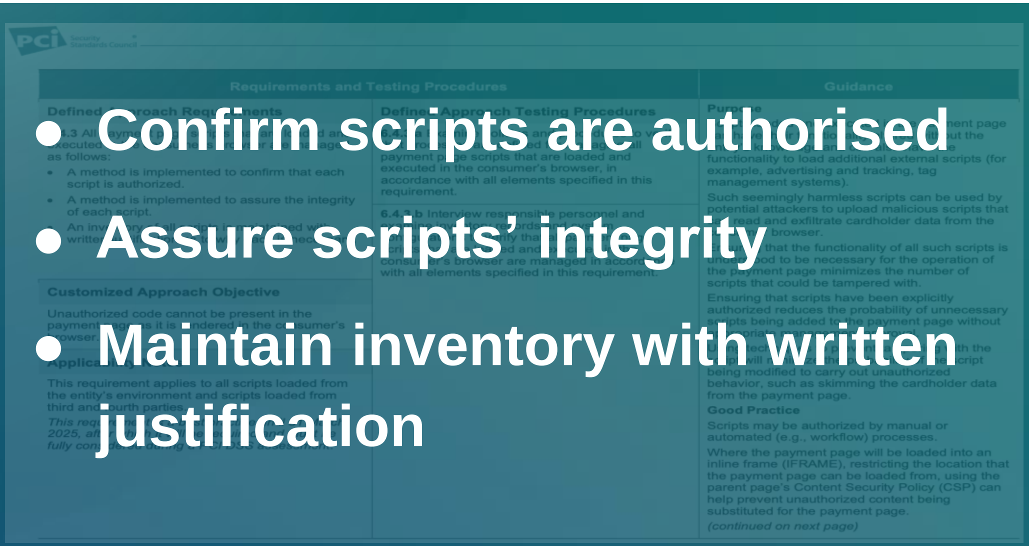
# Enter PCI DSS v4.0

## 6.4.3 & 11.6.1 (primarily)

# In a Nutshell

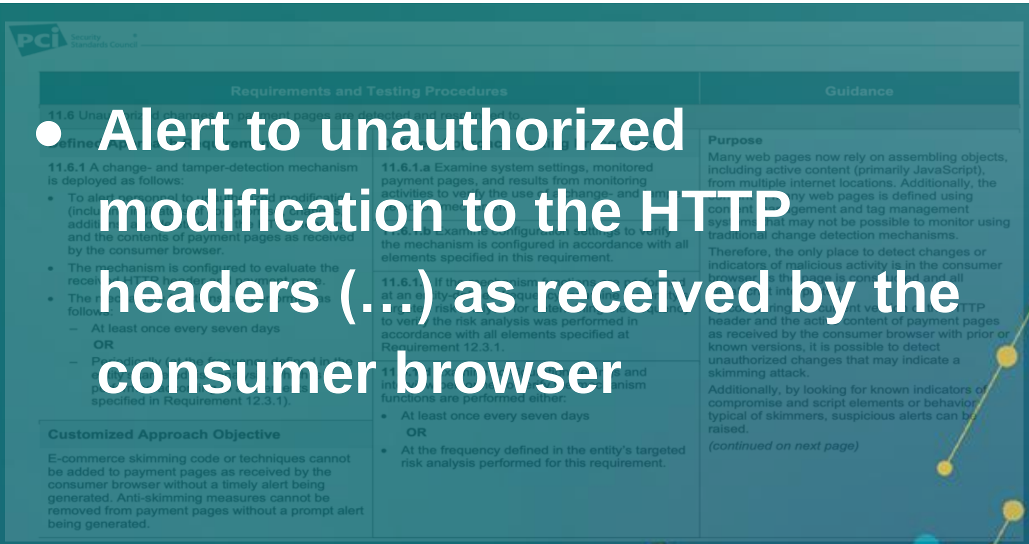
## Goal: Protect cardholder data from payment page browser scripts

### 6.4.3
### Script Management



- Confirm scripts are authorised
- Assure scripts’ integrity
- Maintain inventory with written justification

### 11.6.1
### Change & Tamper Detection



- Alert to unauthorized modification to the HTTP headers (…) as received by the consumer browser

**Deadline: 3/31/2025**

*Reference full requirements in the official PCI DSS 4.0 Doc

# Top Techniques to Protect & Comply

## Avoid cardholder data

# Top Techniques to Protect & Comply

## Avoid scripts

# Top Techniques to Protect & Comply

## Evaluate the options in the standard

### Content Security Policy & Subresource Integrity

Proactive
Free

Complex to manage
Blunt & brittle
No script inventory

### Synthetic Scanner

Inventory/management
Unintrusive

Incomplete & bypassable
Setup & maintenance
Monitoring only

### Real User Monitoring & Defense

Inventory/management
Setup & maintenance
Precision blocking

Yet another script

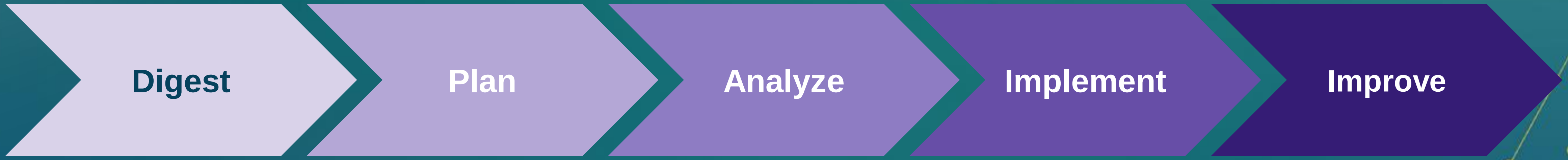
PCI Security Standards Council®

# The Large Enterprise Journey

Steven Eric Fisher, Walmart

*My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.*

# You've Got Work To Do



**Digest**

Know what's coming
Assess risk
Evaluate blast-radius

**Plan**

Map dependencies
Create program
Communicate

**Analyze**

Map current website state
Identify envisioned state & "Pass" State
Design for defense-in-depth
Vet tooling

**Implement**

Address script bloat
Gate 3rd parties
Roll out security tools

**Improve**

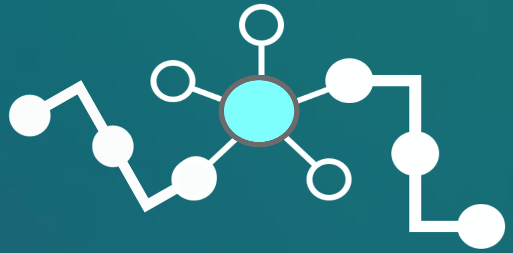
Remediate findings
Simplify architecture
Reduce scope

*My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.*

PCI Security Standards Council®

# Digest

- Journeys start with an origin and a destination
- Nexus – a connection or link between things, especially that is or is part of a chain of causation



*My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.*

# Plan

- 2017-2018 – The rise of the e-skimmers
- App engine native security – was too immature and inconsistent
- Balancing effort, cost, and risk – short term & long term goals

*My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart.*
*They do not reflect the views of Walmart and are not endorsed by Walmart.*

# Analyze

- Engage experts
- Identify script bloat
- Tool up? Identify existing reuse or gap coverage

*My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.*

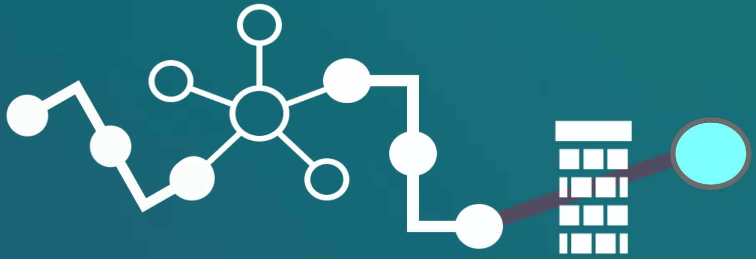
# Implement

- Layer security features
- Controlled gating for 3rd party scripts
- Beware timelines and impacts

*My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.*

# Improve

- Simplify, reduce
- Integrate, automate



*My presentation, comments and opinions are provided in my personal capacity and not as a representative of Walmart. They do not reflect the views of Walmart and are not endorsed by Walmart.*

# Key Takeaways

1. New payment page protection requirements (6.4.3 & 11.6.1) address an important security gap, but effective implementation can be challenging for enterprises

2. Large enterprises should start ASAP with scoping, aligning stakeholders and process, and deploying technology that can balance security and business needs

3. We recommend engaging expertise, layering multiple technical & process controls, and seeking opportunities to simplify and automate with maturity

# Thank you!

PCI Security Standards Council®