

# **RSAC**Conference2020

San Francisco | February 24 – 28 | Moscone Center

**HUMAN**  
ELEMENT

SESSION ID: DSO-W02

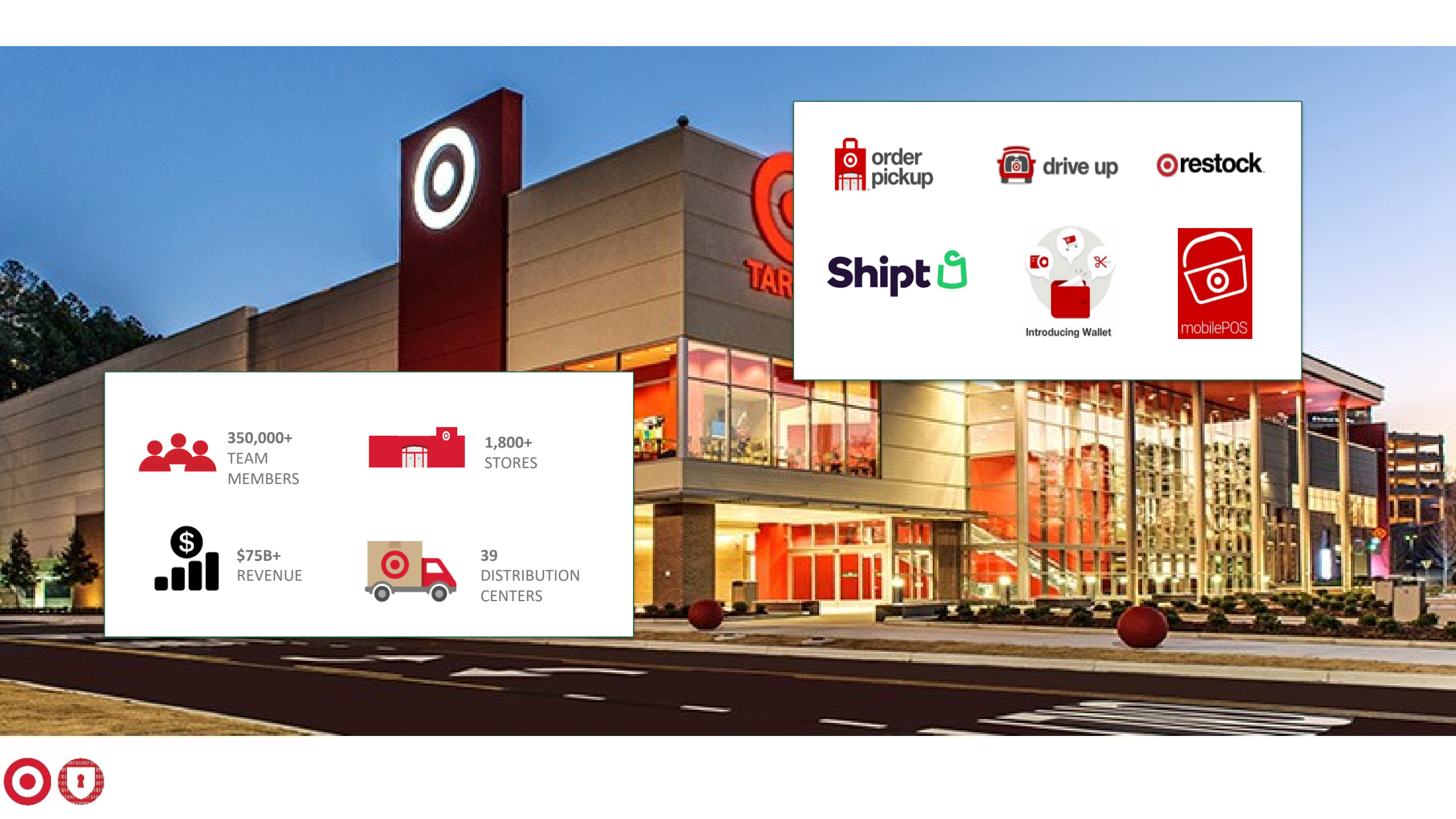
## When Application Security “The Wrong Way” Is the Right Thing for Your Organization



**Jennifer Czaplewski**

Director, Product Security  
Target

#RSAC



Introducing Wallet



350,000+  
TEAM  
MEMBERS



1,800+  
STORES

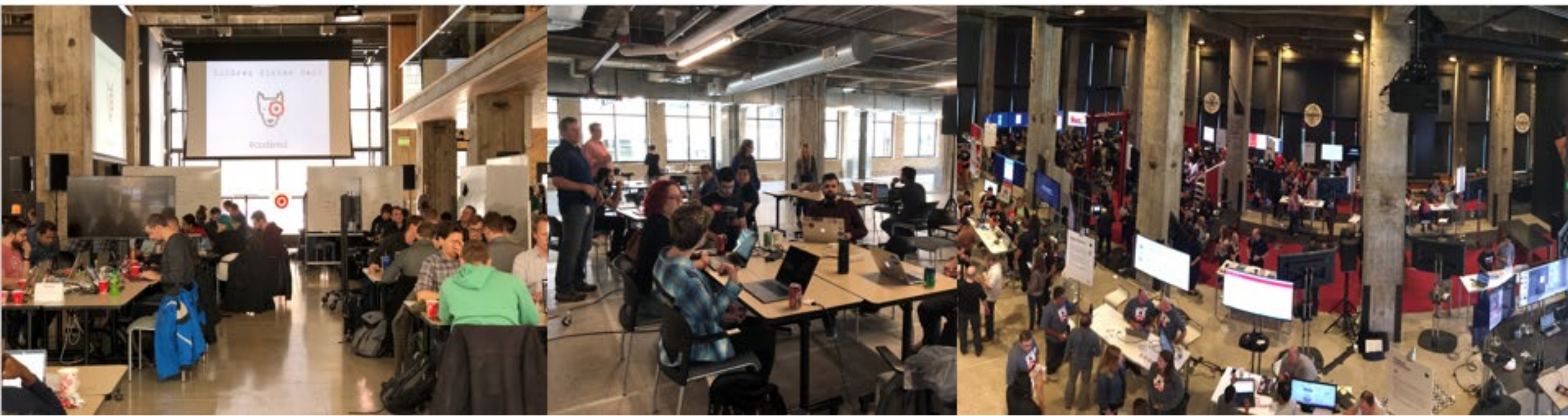


\$75B+  
REVENUE



39  
DISTRIBUTION  
CENTERS





- ✓ **Organize:** Product model, Agile, DevOps
- ✓ **Build:** Shift from packages to in-house engineering
- ✓ **Fail fast:** Innovation and continuous learning

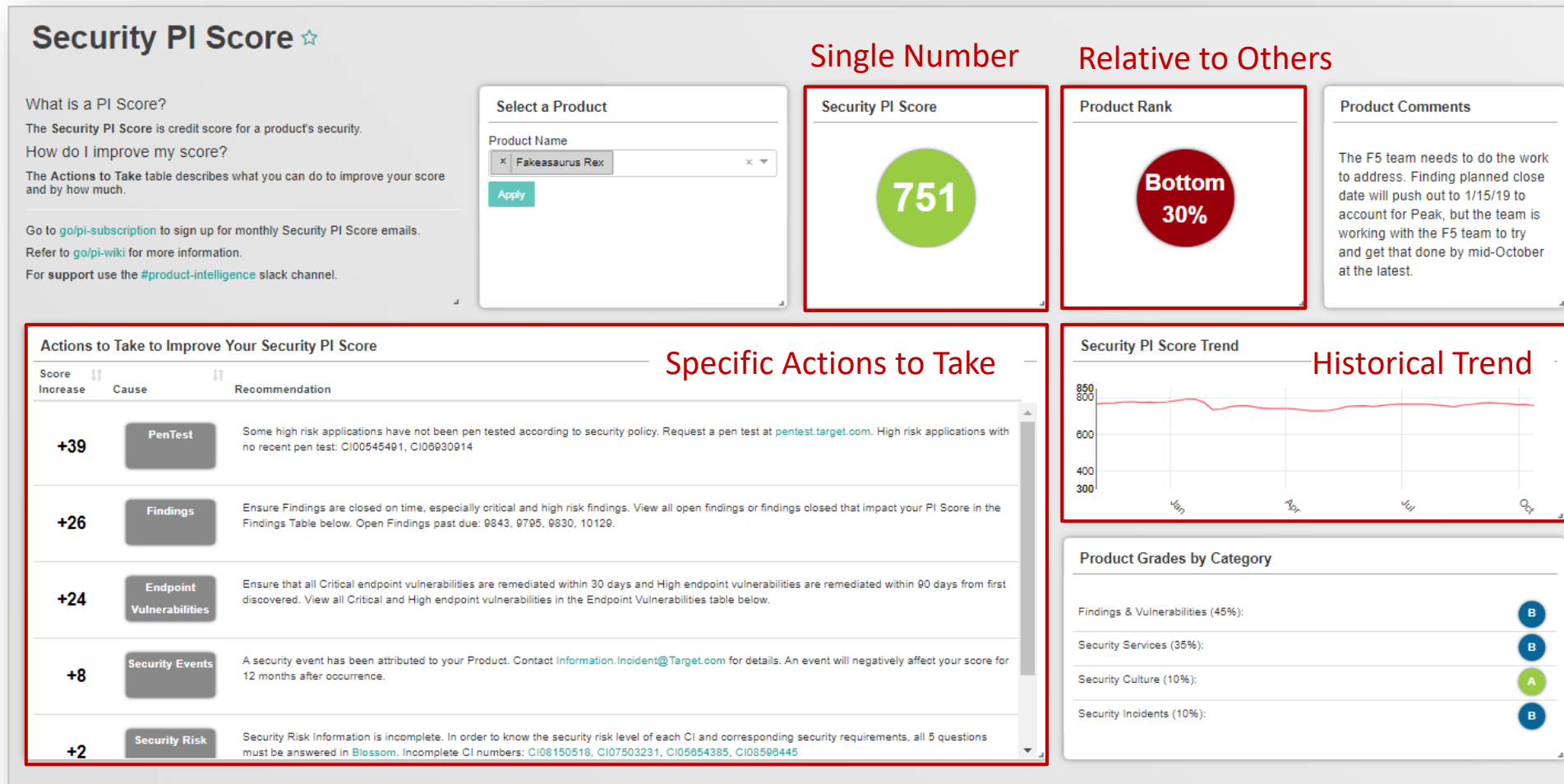


**RSA**®Conference2020

**Myth: There's no single metric to  
measure application security**



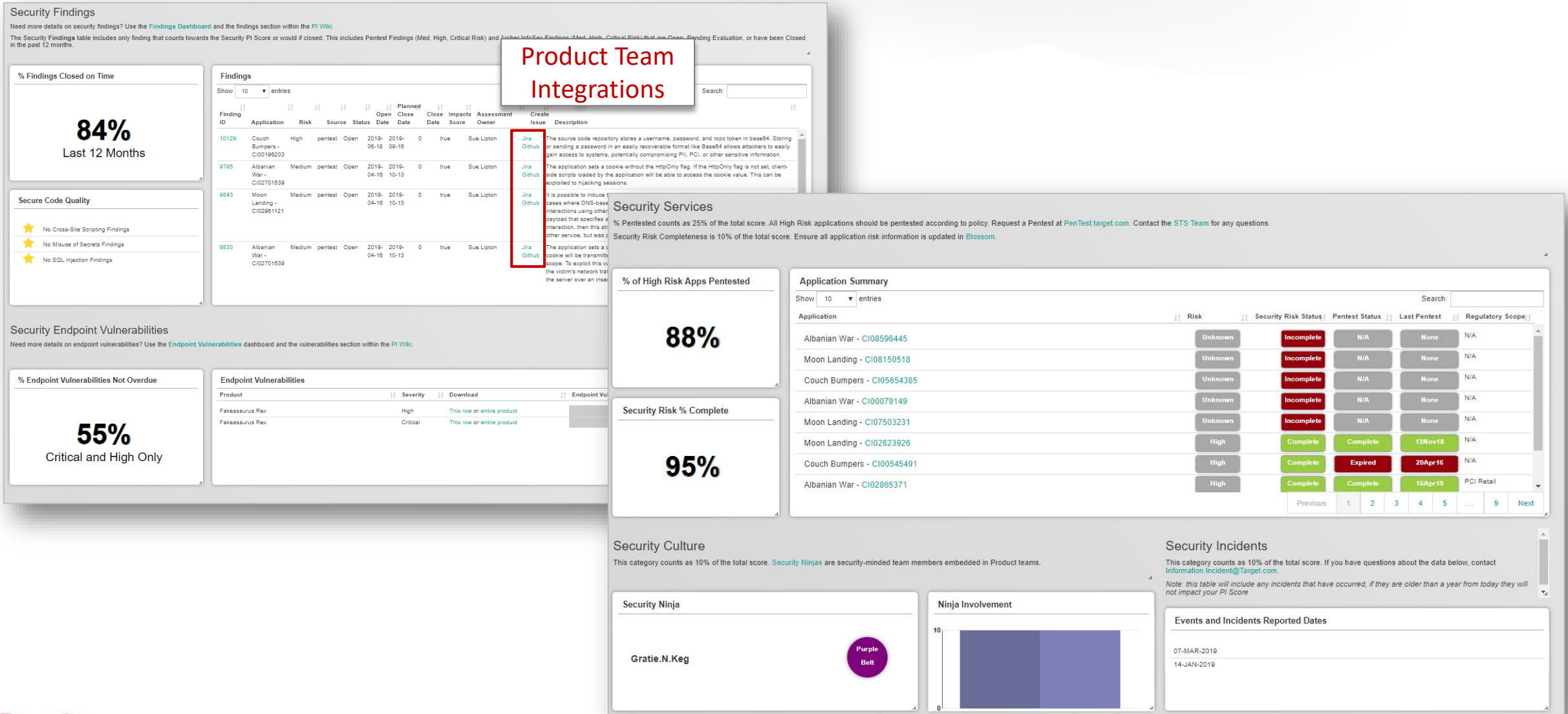
# Product Intelligence



1. Findings and Vulnerabilities (45%)
2. Security Services (35%)
3. Security Culture (10%)
4. Security Incidents (10%)

On time closure (e.g. audit findings, pen test findings)  
Must use required services (e.g. penetration testing)  
e.g. Security Ninja appointed and attending trainings  
e.g. Product has been root cause of a security incident

# Product Intelligence



# Product Intelligence

## Portfolio Security Summary ☆

### Select a Portfolio

Portfolio Name

✕  ✕

Apply

### Key Metrics

Security Risk % Complete 95%

High-Risk Apps % Pentest Complete 76%

12 Month % Findings Closed on Time 75%

% Endpoint Vulnerabilities Not Overdue 48%

SQL Injection (SQLi) Findings 0

Cross-Site Scripting (XSS) Findings 0

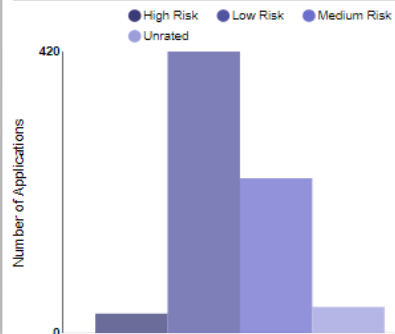
Misuse of Secrets Findings 0

### Product List

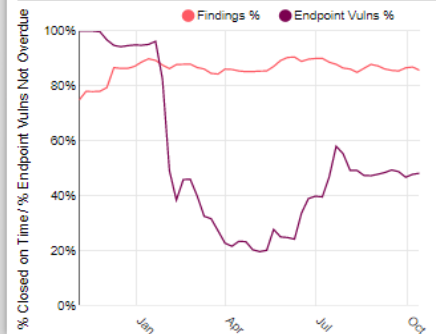
Search: 

Product Name	PI Score	Percentile	Security Ninja	Comments
Bogusiosarus	564	Bottom 10%	Ninja Needed	
Shamomimus	722	Bottom 20%	Sue.Lipton	
Fakeasaurus Rex	751	Bottom 30%	Gratie.N.Keg	The F5 team needs to do the work to address. Finding planned close date will push out to 1/15/19 to account for Peak, but the team is working with the F5 team to try and get that done by mid-October at the latest.
Erroneousaurus	780	Bottom 50%	Chuck.Norris	
Untroodon	802	Upper 40%	Kris.Lindahl	

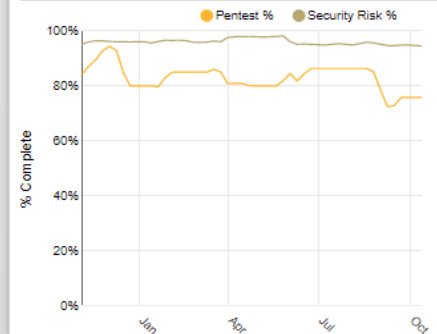
### Portfolio Applications by Risk



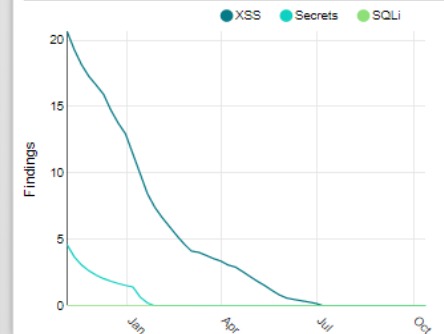
### Findings and Endpoint Vulnerabilities - Trend



### Security Services - Trend



### Secure Coding - Trend



# *What you need to build your own*

## Technology

- ✓ **Resources:** 2-3 for build and ongoing support
- ✓ **Technology:** Can be mostly done with Open Source
- ✓ **Integrations:** Most source systems have good APIs

## Prerequisites

- ✓ **Asset Management:** Basic awareness of assets
- ✓ **Clear policy:** Requirements and risk rating structure
- ✓ **Top Down Commitment:** Not “just another metric”





# **RSA**Conference2020

**Myth: Welcome any and all engineers to a security guild. Better still, mandate participation**

# Target's *Exclusive* Security Ninja Program

## Participants are

- Seasoned
- Influential
- Passionate

## Program is

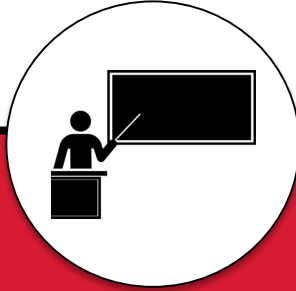
- Exclusive (<5% of tech population)
- Builds security awareness & excitement
- Accidental talent pipeline



# Security Ninja Responsibilities



Build and maintain  
security knowledge



Guide teams in  
security best practices



Maintain application  
inventory data



Voice of customer for  
Info Security



# Security Knowledge Development

## Initial Onboarding



- Security Fundamentals
- Hands on Hacking

## Monthly Information Sharing



- Topic deep dives
- Identify actions
- ChatOps

## Quarterly Hands On Events



Interactive  
events for  
deeper learning

## Elevated Belts



Opportunities to earn  
Purple or Black Belt

# Organization-wide impact

"My team cares more about security; they've done better considering security earlier than they used to"



"Our ninja influences team culture towards a security aware mindset; she helps to articulate risk, prioritize resolution and educate the team"



"The way our team thinks about security today is different than before we had our Security Ninja; our security culture is more mature"



"It's helped me get over my imposter syndrome and realize I am pretty good at security stuff, and I know what I'm talking about!"



Rate the effectiveness of your security ninja:

79% Effective  
or Very Effective





**RSA**®Conference2020

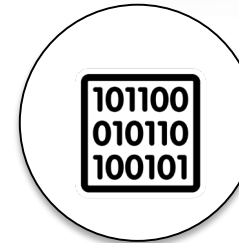
**Myth: Scan ALL the things**

# Spotlight SAST

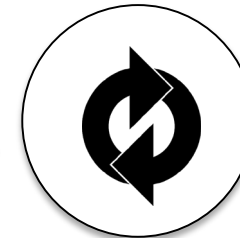
## Objective

*Improve application security by integrating SAST into engineering practices*

## Values



Meet developers where they work



Offer end to end solutions




“Right way” = easiest way



# Spotlight SAST User Experience

## Spotlight SAST


[#spotlight-sast](#)
[i docs](#)
[onboard](#)

You can use this UI to configure how you would like to receive feedback for issues found in Spotlight SAST scans. You will ONLY be able to mark false-positives using GitHub issues or JIRA stories. We recommend that you DO NOT make Spotlight SAST a required check in your GitHub code review process.

[Disable All in View](#)
[Enable All in View](#)
[Enable All in View](#)
[Bulk Edit Jira Project For All in View](#)

Owner	Repository	CI	Email Enabled	Email Upon Successful Scan	GitHub Issues Enabled	JIRA Stories Enabled
			All   v	All   v	All   v	All   v
JenniferCzaplewski	<a href="#">cicd_workshop</a>	Enter CI or application...   v	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Enter JIRA project...   v
JenniferCzaplewski	<a href="#">Czaplewski_Team_Repo</a>	Enter CI or application...   v	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Enter JIRA project...   v
JenniferCzaplewski	<a href="#">Goals-and-Objectives</a>	Enter CI or application...   v	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Enter JIRA project...   v
JenniferCzaplewski	<a href="#">Ninjas</a>	Enter CI or application...   v	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Enter JIRA project...   v
JenniferCzaplewski	<a href="#">PSE-ToolsStrategy</a>	Enter CI or application...   v	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Enter JIRA project...   v
JenniferCzaplewski	<a href="#">security-portal</a>	Enter CI or application...   v	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Enter JIRA project...   v
JenniferCzaplewski	<a href="#">TestRepo.md</a>	Enter CI or application...   v	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Enter JIRA project...   v
JenniferCzaplewski	<a href="#">Training</a>	Enter CI or application...   v	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Enter JIRA project...   v



## Version 1

vs

## Version 2

Provide separate ticket/email  
for each issue in each branch

Issues



Reduce noise through  
consolidated tickets/emails

Unpredictable notifications

Notices



Customer-focused notifications

Users either fix or mark as  
false positive

Status



More granular response  
beyond false-positive

Short description about how  
to resolve

Fix



Improved information about  
resolution guidance



# **RSA**®Conference2020

## **Learnings**

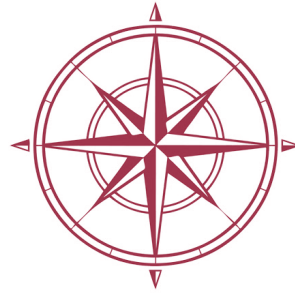


# Lessons Learned



## Iterate Iterate

Define your MVP  
and build from there



## Focus on Behavior

Our guiding principle:  
“what behavior do we want to drive”



## Keep it Simple

Less is usually more

# Apply What You Have Learned Today

- Next week you should:
  - Meet with your customers!
  - Identify 3 desired customer behaviors
- In three months:
  - Develop *objective* (not subjective) measurements
  - *Simplify* at least 3 metrics
  - Define *your* MVP...and build it
  - Meet with your customers (again)
- In six months:
  - Meet with your customers!
  - Iterate and improve your MVP based on measurements and behaviors



# RSA®Conference2020

Thank you!

Questions??

