

# ADD0

ALL DAY DEVOPS

NOVEMBER 6, 2019

Jennifer Czaplewski

## Security Data: GPS for Application Teams













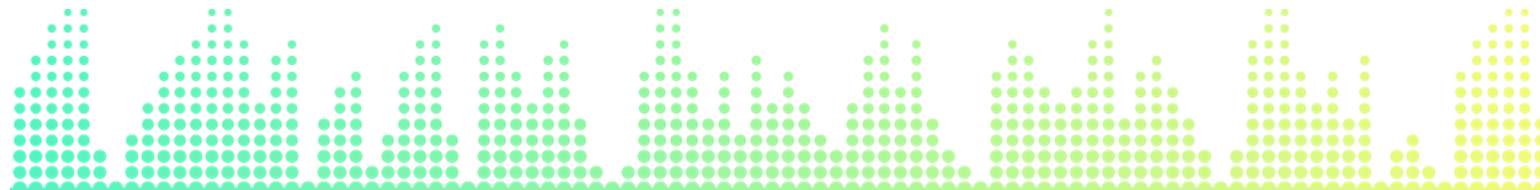
A photograph of a Target retail store at night. The building is illuminated, showing the large Target bullseye logo on a tall sign and the word 'TARGET' in red letters on the facade. The store has large glass windows reflecting the street lights. In the foreground, there is a parking lot with some red spherical planters.

	350,000+ TEAM MEMBERS		1,800+ STORES
	\$70B+ REVENUE		39 DISTRIBUTION CENTERS

 order pickup	 drive up	 restock
 SHIPT™	 Introducing Wallet	 mobilePOS



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







## *Security as the enforcer*



## *Security as the teacher*

### Guidance



Policy = “do this but you figure out how”

Easily consumable services and patterns  
Business Partnerships

### Education



Assigned online/classroom training

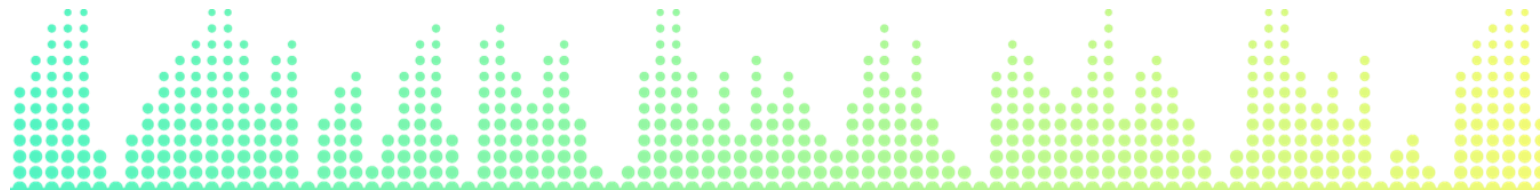
Relevant, on-demand, social learning

### Tools



Request code-scans and testing

Self-service, integrated in the pipeline



## Doing the right thing is hard when it's not clear what "right" means



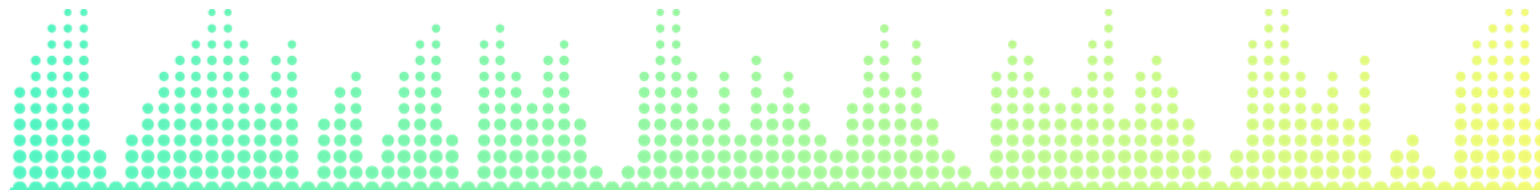
Remind you of  
your policy?

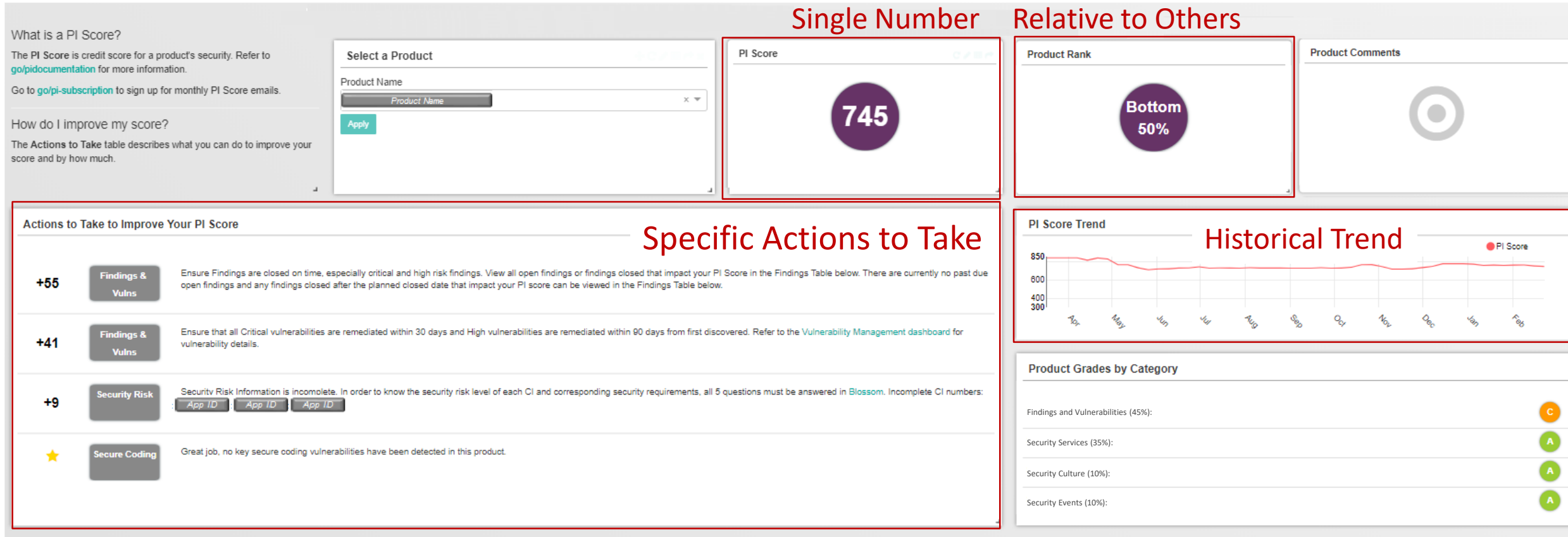


Conflicting guidance  
from your own team?



The same ... or  
different opinions?





**1. Findings & Vulnerabilities (45%)**

**2. Security Services (35%)**

**3. Security Culture (10%)**

**4. Security Events (10%)**

On-time closure (e.g. audit findings, vulns, pen test findings etc.)

Must use required services (e.g. completed annual pen test?)

e.g. Security Ninja appointed and attending trainings?

e.g. Product has been root cause of a recent security event

## Security Findings

### % Findings Closed on Time

**100%**  
Last 12 Months

### Secure Code Quality

- ★ No Cross-Site Scripting Findings
- ★ No Misuse of Secrets Findings
- ★ No SQL Injection Findings

### Findings

Show 10 entries

Search:

Finding ID	Application	Risk	Source	Status	Open Date	Planned Close Date	Close Date	Is Scorable	Assessment Owner	Create Issue	Description
7											
7											

## Security Services

### % of High Risk Apps Pentested

**100%**

### Security Risk % Complete

**100%**

### Application Summary

Show 10 entries

Search:

Application	Risk	Security Risk Status	Pentest Status	Last Pentest
	High	Complete	Complete	21Dec17
	Medium	Complete	Complete	12Nov18
	Medium	Complete	N/A	None
	Medium	Complete	N/A	None
	Medium	Complete	Complete	02May17
	Medium	Complete	N/A	None
	Medium	Complete	N/A	None
	Medium	Complete	N/A	None

Previous 1 2 3 4 5 Next



## Portfolio Security Summary ☆

Actions ▾

### Select a Portfolio

Portfolio Name

Security

X ▾

Apply

### Key Metrics

Security Risk % Complete

High-Risk Apps % Pentest Complete

12 Month % Findings Closed on Time

% Vulnerabilities Not Overdue

SQL Injection (SQLi) Findings

Cross-Site Scripting (XSS) Findings

Misuse of Secrets Findings

### Product List

Product Group Name

Product Name

PI Score

Security Ninja

Percentile

Search:

Comments

Security Solutions

680

Bottom 20%

Security Solutions

724

Bottom 30%

Security Solutions

739

Bottom 40%

Security Solutions

740

Bottom 40%

Cyber Security

744

Bottom 40%

Security Solutions

759

Bottom 50%

Security Solutions

762

Bottom 50%

Security Solutions

764

Bottom 50%

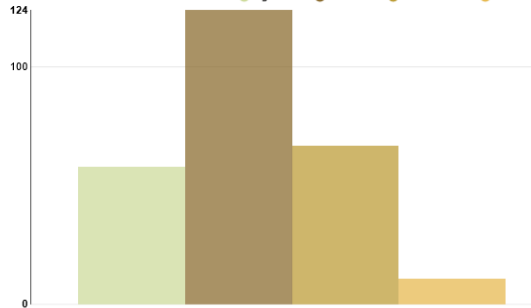
Security Solutions

776

Upper 50%

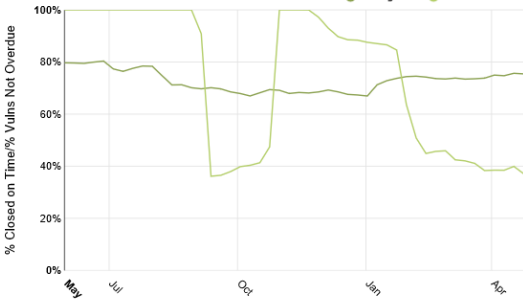
### Portfolio Applications by Risk

High Risk Low Risk Medium Risk Unrated



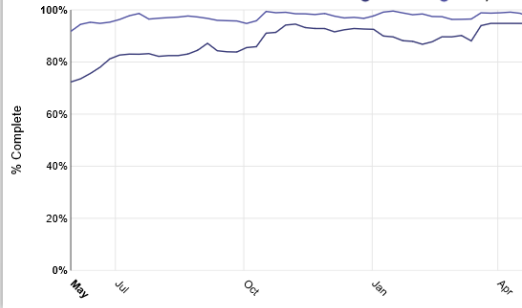
### Findings and Vulnerabilities - Trend

Findings % Vulnerabilities %



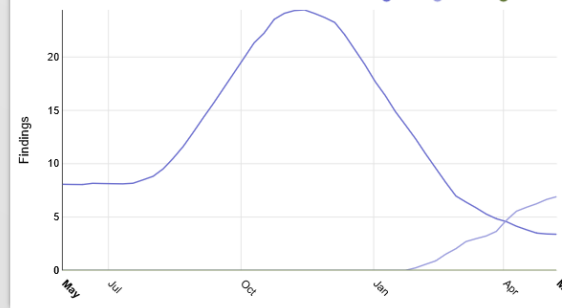
### Security Services - Trend

Pentest % Security Risk %



### Secure Coding - Trend

XSS Secrets SQLi







## Iterate Iterate

Define your MVP and  
build from there



## Focus on Behavior

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



## Use Competition

Teams see their  
score compared to  
others



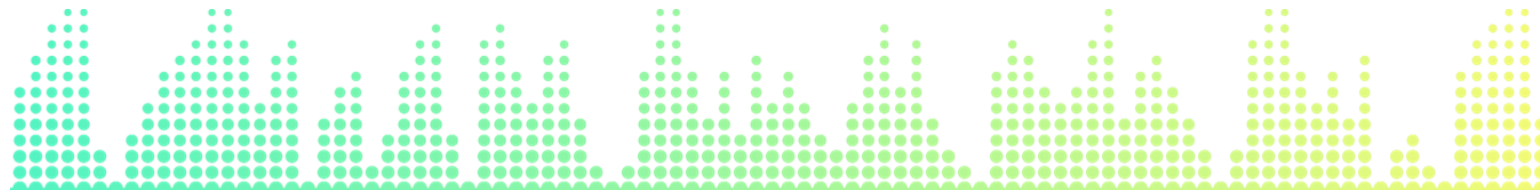
## Keep it Simple

Less is  
usually more



## Data Accuracy

Real or  
perceived

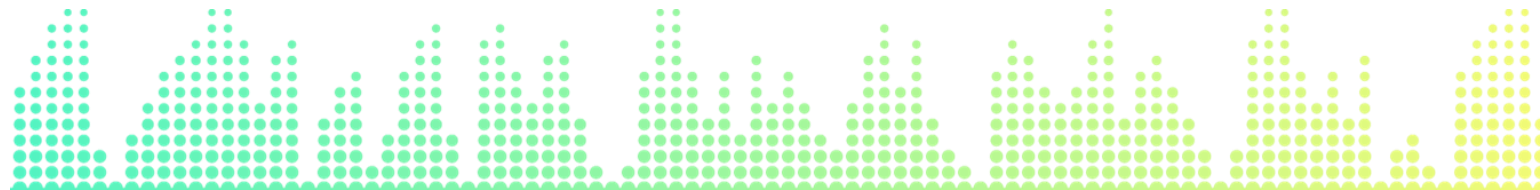


## Technology

- ✓ **Resources:** 2-3 for build and ongoing support
- ✓ **Technology:** Can be mostly done with Open Source
- ✓ **Integrations:** Data exists in source systems

## Prerequisites

- ✓ **Asset Management:** At minimum, application awareness
- ✓ **Clear policy:** Requirements and risk rating structure
- ✓ **Top Down Commitment:** Not “just another metric”



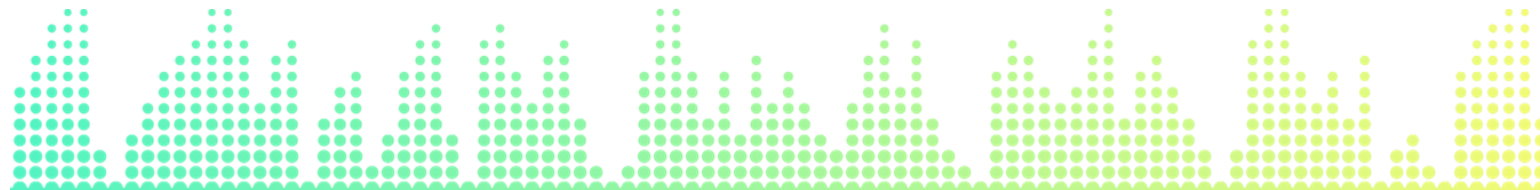
## Security Ninjas



## Business Information Security Office



## Dev & Ops PI's





# Questions?

## See you on Slack!

