NINTH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

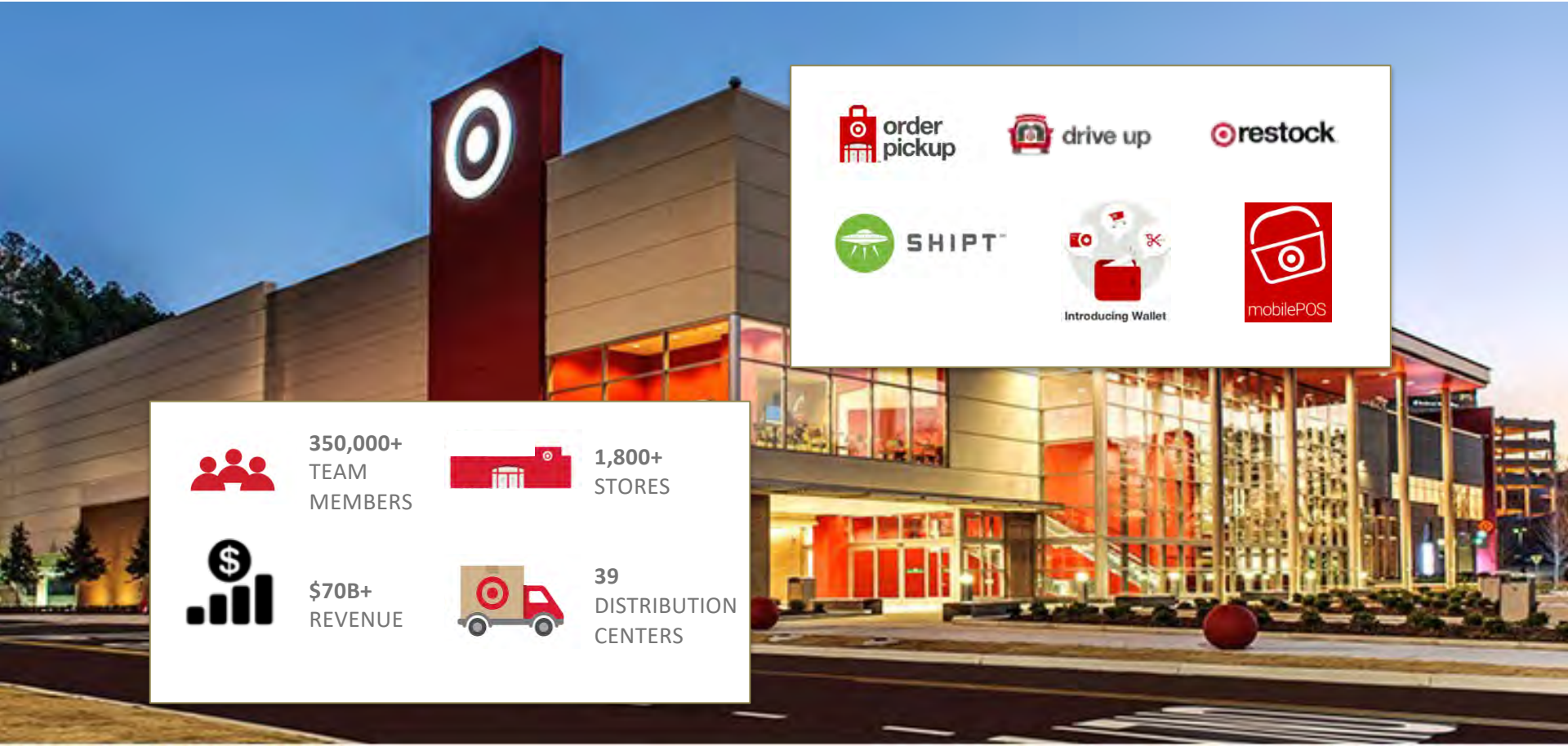
Security solutions through collaboration.™

October 28–30, 2019 | Minneapolis Convention Center

cybersecuritysummit.org | #cybersummitmn

Security Data: GPS for Application Teams

Jennifer Czaplewski
Director, Product Security at Target


order pickup
drive up
restock
SHIPT
Introducing Wallet
mobilePOS
350,000+ TEAM MEMBERS
1,800+ STORES
$70B+ REVENUE
39 DISTRIBUTION CENTERS

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

Shifting the Security Culture

	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

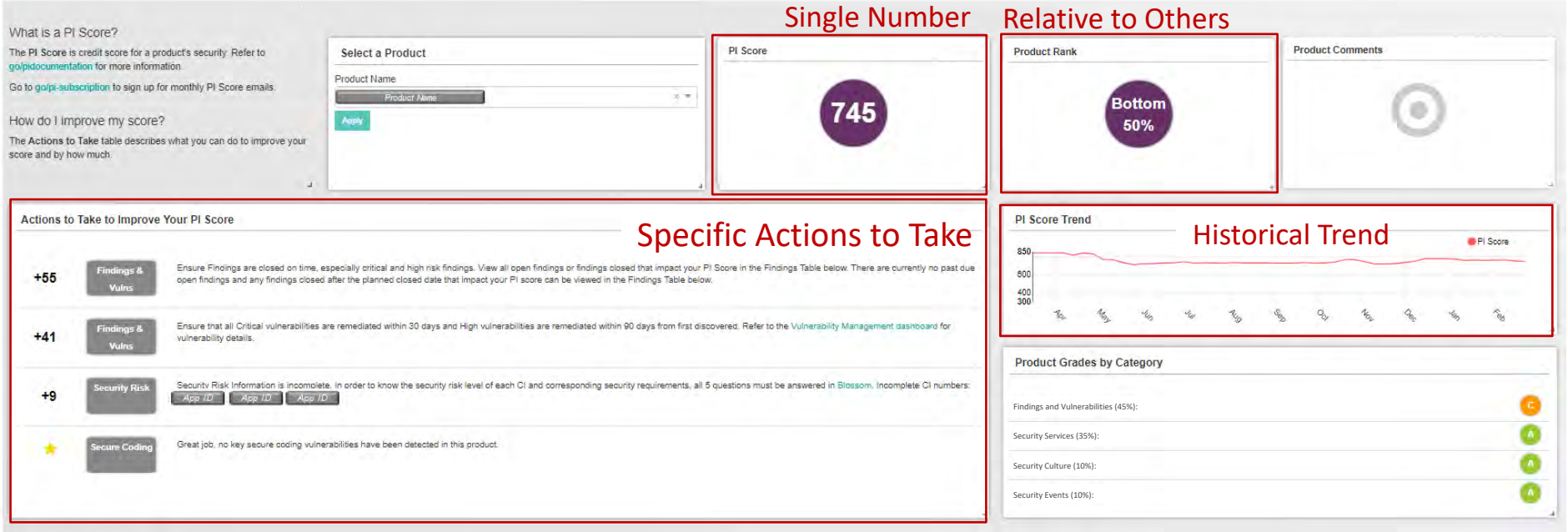
Doing the right thing is hard when it's not clear what "right" means

Remind you of your policy?

Conflicting guidance from your own team?

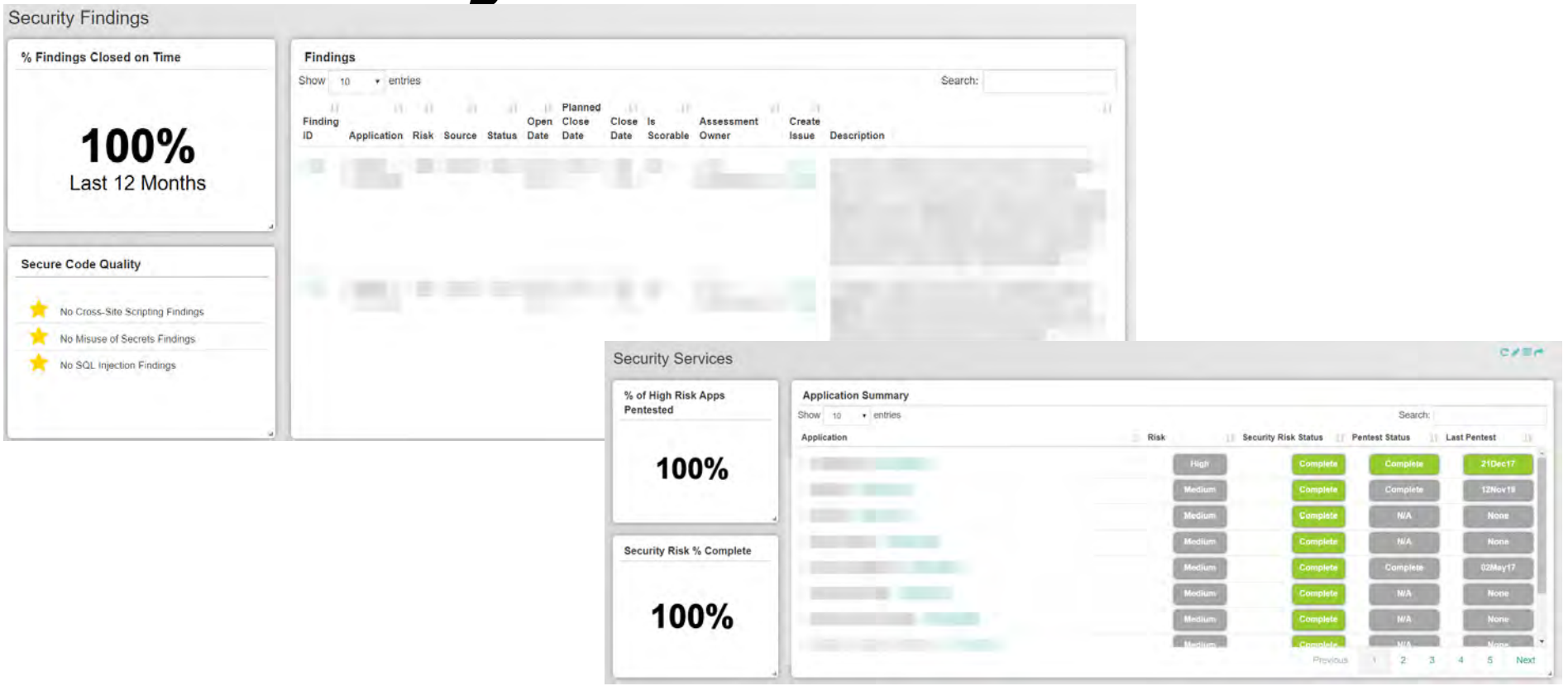
The same … or different opinions?

Product Intelligence

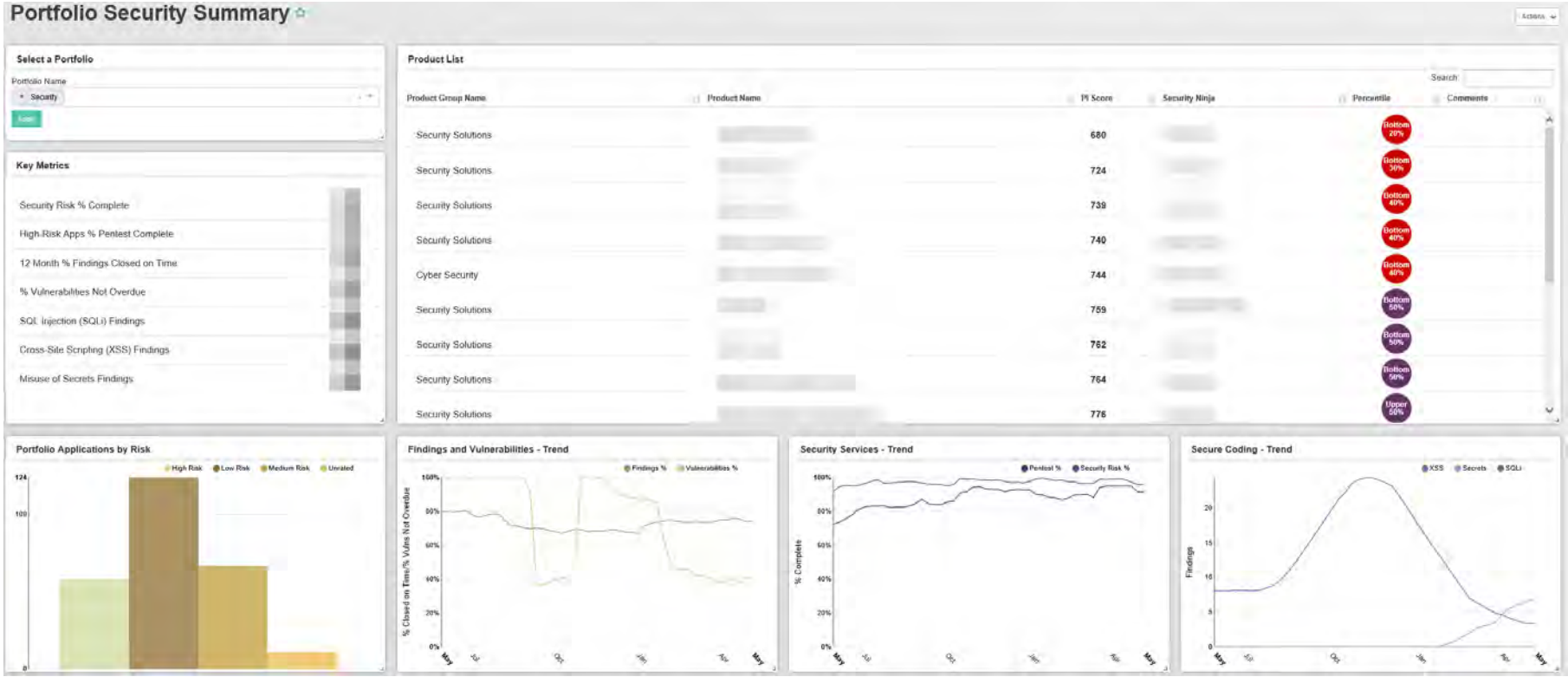


1. Findings & Vulnerabilities (45%)	On-time closure (e.g. audit findings, vulns, pen test findings etc.)
2. Security Services (35%)	Must use required services (e.g. completed annual pen test?)
3. Security Culture (10%)	e.g. Security Ninja appointed and attending trainings?
4. Security Events (10%)	e.g. Product has been root cause of a recent security event

Product Intelligence - Details



Leader View


Portfolio Security Summary
Select a Portfolio
Portfolio Name
Security
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
Search
Product Group Name
Product Name
PI Score
Security Ninja
Percentile
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 %
% Closed on Time/% Vulns Not Overdue
Security Services - Trend
Pentest %
Security Risk %
% Complete
Secure Coding - Trend
XSS
Secrets
SQLi
Findings

Lessons Learned

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

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:** 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"

Continued Cultural Integration

Security Ninjas

Business Information Security Office

Dev & Ops PI's

Questions?