WHAT KEEPS YOUR SOFTWARE VENDORS UP AT NIGHT?

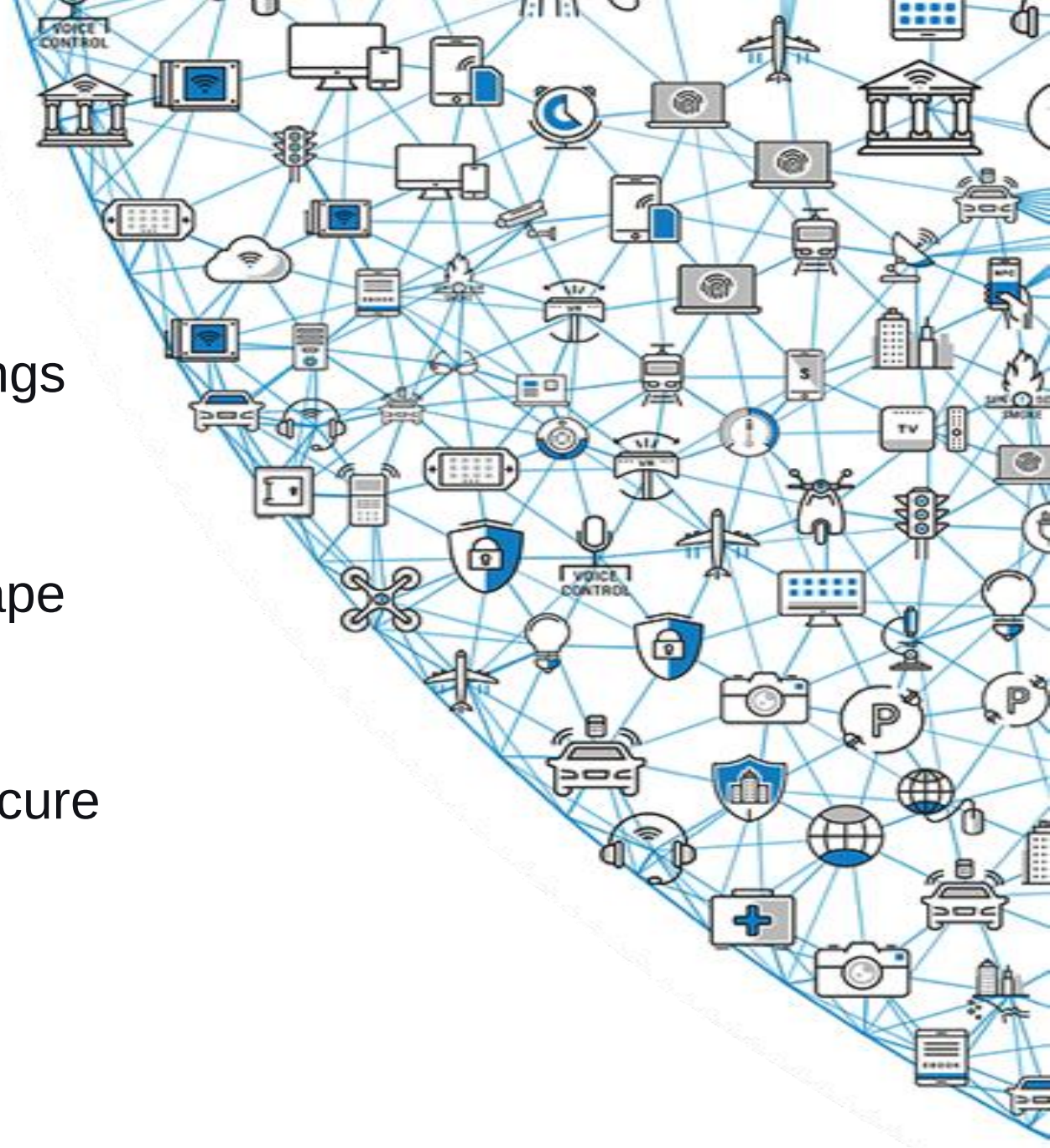
Tyler Townes

BlackBerry

September 2018

Agenda

1. Who am I?
2. BlackBerry and the Enterprise of Things
3. Product Security and the SDLC
4. The Product Security Threat Landscape
5. What you can do to make sure your software vendors are keeping you secure



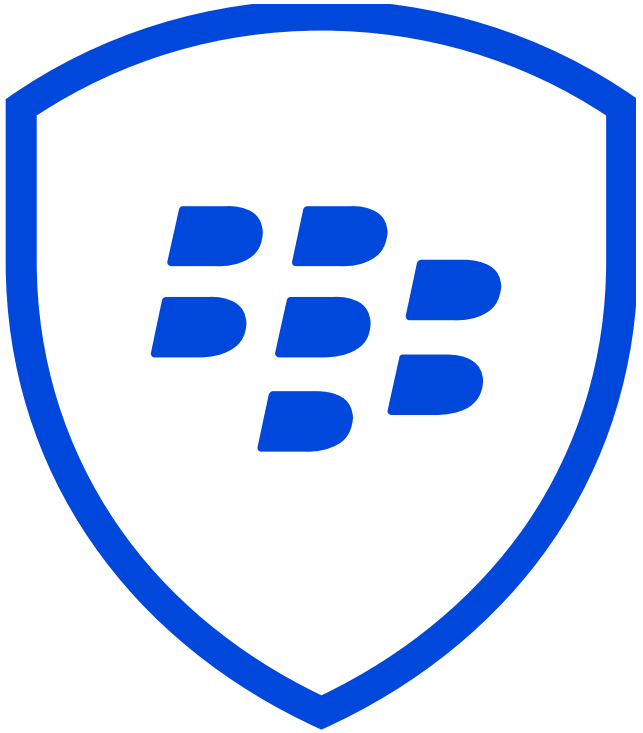
Who am I?

5 years at **BlackBerry Product Security**

BlackBerry Product Security Response Leader

- Incident Response
- Vulnerability Management
- Risk Assessment
- Coordinated Disclosure
- Ecosystem Threat Management

Mobile malware / Spy ware investigator



This is what keeps me up at night

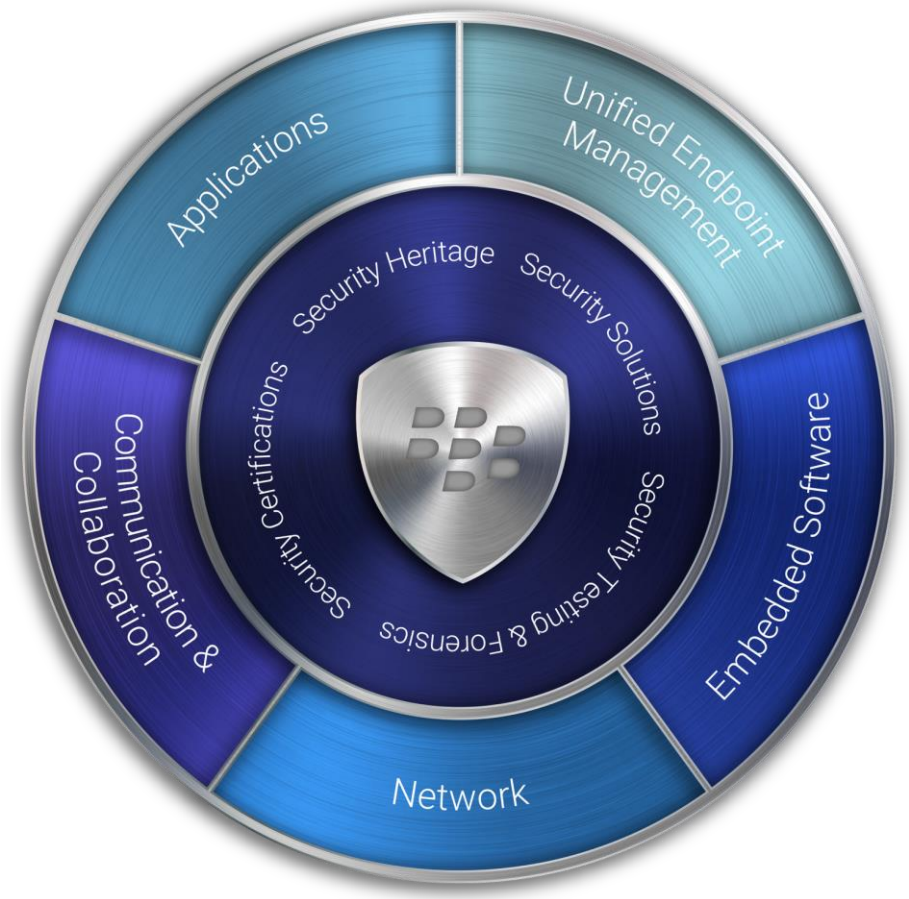
8,000 pieces of threat intel investigated

650 cases investigated

10,000 vulnerabilities investigated

9 advisories released

BlackBerry Secure and the Enterprise of Things



Software/Secure Development Lifecycle

Software Development

Product Security

How do you discover Product Security threats?

Hacking Forums	Academic White Papers
Conference Presentations	Linux Distribution Advisories
Enterprise Customers	Twitter
End Users	openwall
Google Alerts	bugtraq
Media	Mitre
Open Source Alerts	ZDI
Mailing Lists	Professional Network

Open Source Software (OSS) as an attack surface

- Monitoring **600+ unique OSS libraries**

- **7,000 unique vulnerabilities** reported this year impacting those 600 libraries

- **No set release schedule** for OSS vulnerability notifications

Software vendors being bitten by out of date OSS

- Popular Anti-Virus products being **shipped** with components containing **7 year out of date** OSS libraries
- Dozens of vulnerabilities with **public exploits!**
- https://googleprojectzero.blogspot.ca/2016/06/how-to-compromise-enterprise-endpoint.html

The Security Questionnaire

- Comprehensive for Network Security, Governance, Risk, and Compliance
- Often lacking Product Security questions
- Questionnaire reflects the organization who’s delivering it

Does this keep your software vendor up at night?

- What actions do you perform in each phase of the **Software Development Life Cycle?**
- What is your **Incident Response plan?**
- Are you using **upstream components?**
- How will you **inform me** if there is a **risk** to my deployment?

Summary

Product Security is a core element of an organization’s security posture

Hold your vendors accountable for the security of the products that you deploy

@tyler_townes
ttownes@blackberry.com
Github.com/productsecurity

BlackBerry