Lessons Learned from Securing MPoC Solutions

Need for Continuous Security

Agenda

1. Intro
2. Evolution of MPoC
3. Risks with COTS devices
4. Certification vs. Continuous Security
5. Lesson Learned
    - Challenges
    - Best Practices

PCI Security Standards Council

About Zimperium

Securing mobile applications & devices since 2009

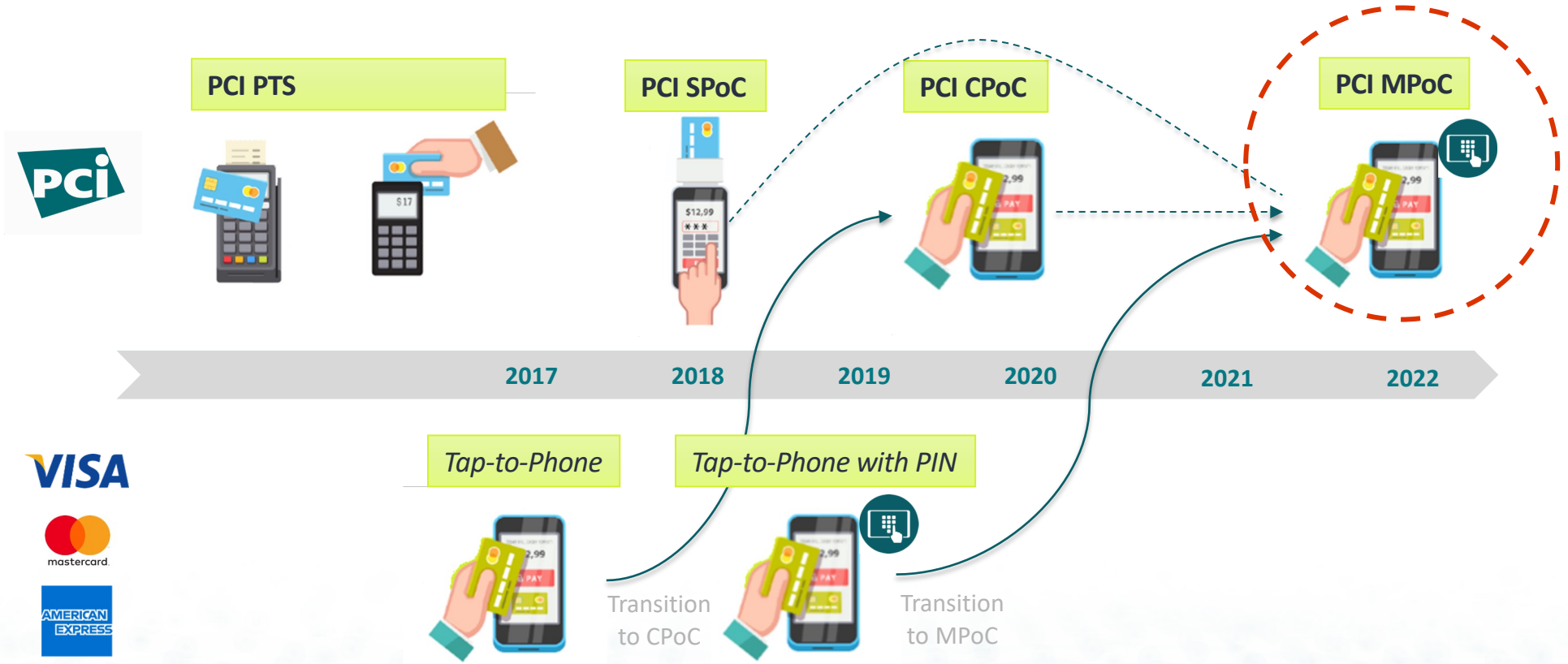
Securing leading Mobile Wallet and SDK solutions since 2014

Securing the leading certified EMVCo SBMP, PCI SPoC and CPoC solutions

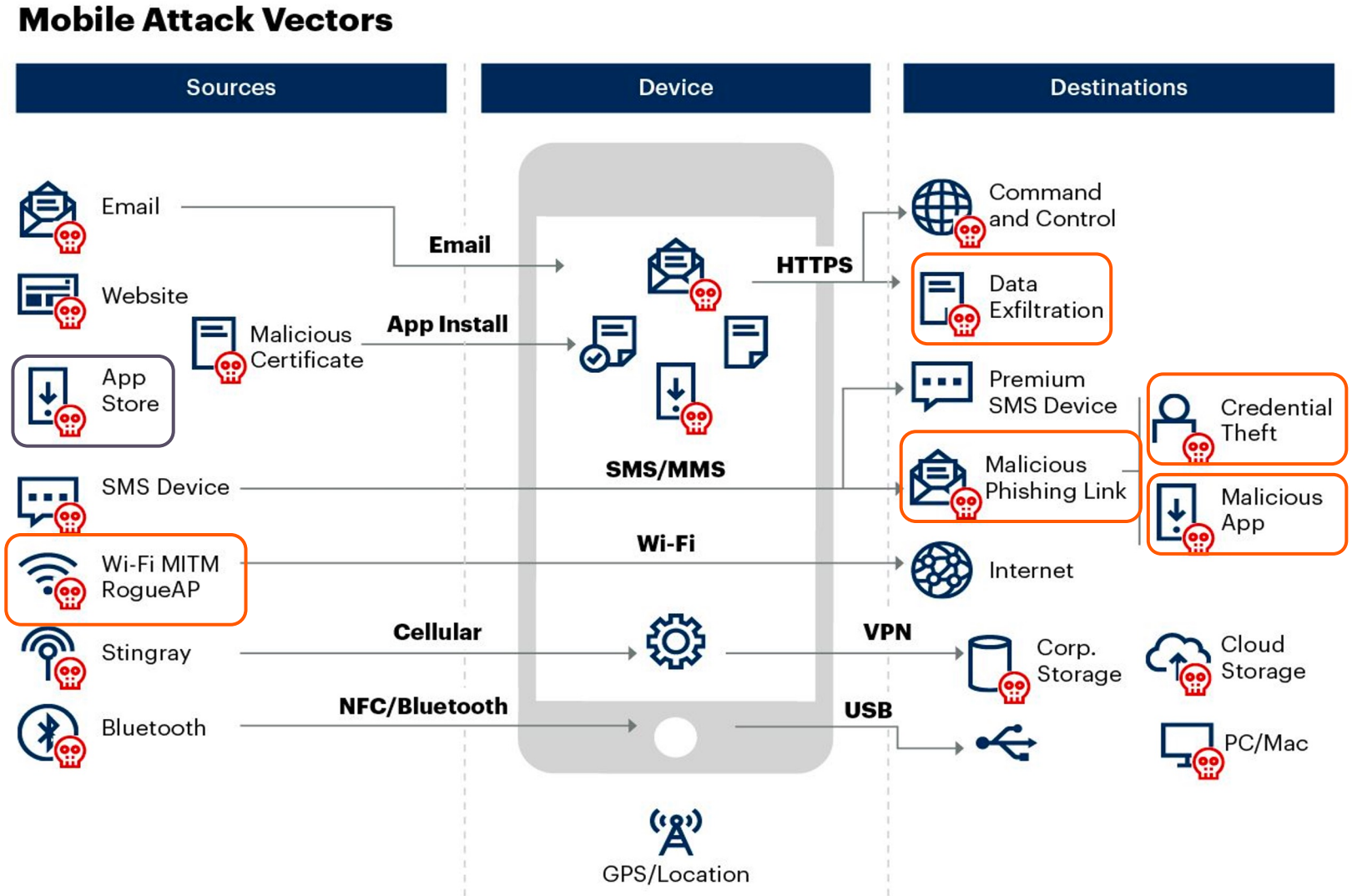
Supporting 30+ SoftPOS and HCE developers worldwide

PCI Security Standards Council

Evolution To MPOC



The problem with COTS mobile devices



MITM = man in the middle; NFC = Near Field Communication

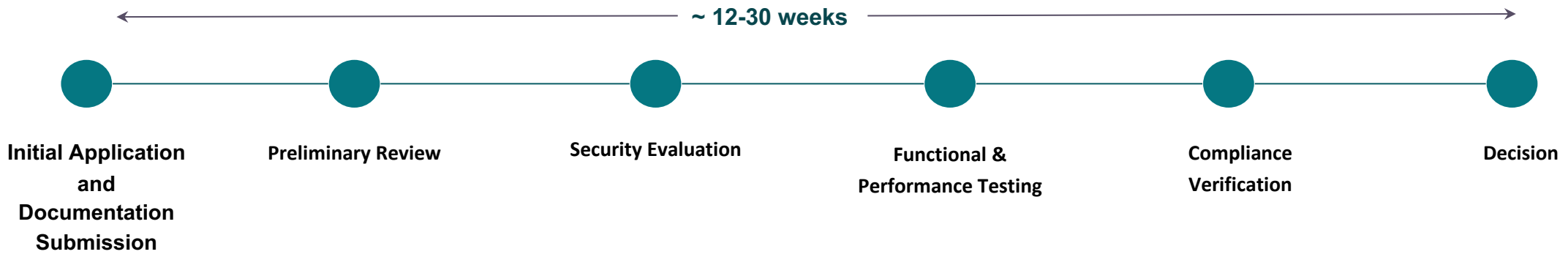
Source: Gartner

775183_C

PCI Security Standards Council

Gartner

Certification vs. Continuous Security



Once the app is released, the real threat begins

Attacker Tools Become More Sophisticated	Sophisticated Malware Variants Emerges	Supply Chain Risks Emerge	New Zero-Day Vulnerabilities Discovered	Continuous Platform Updates Published

PCI Security Standards Council®

Advanced Attacker Tooling

Evolving Threat Landscape

Magisk | Rooting Tool

- Systemless Rooting
- Evade SafetyNet
- Evasion
- Persistence

Active Community

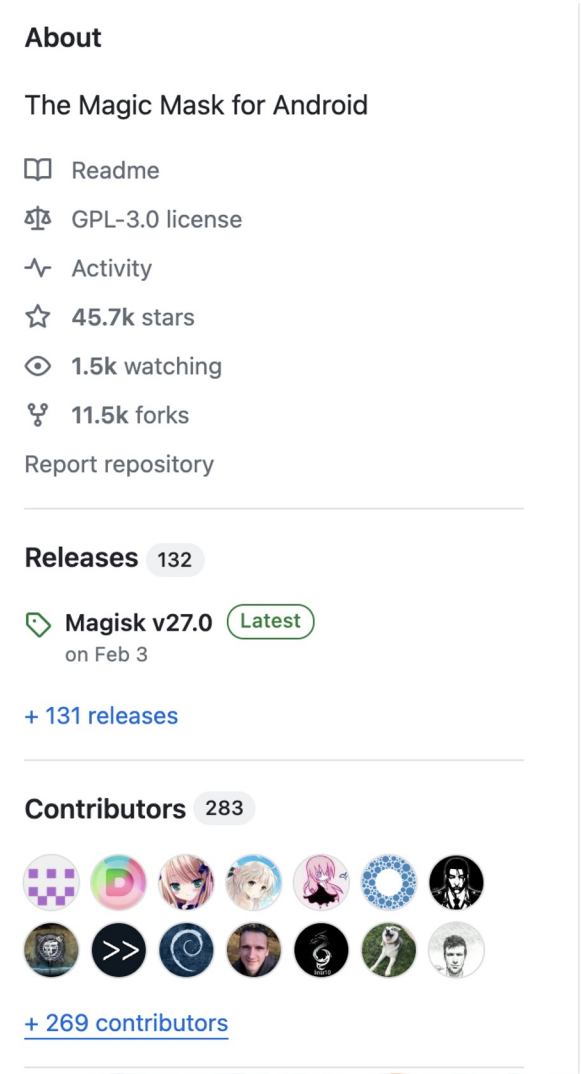
- **283 Contributors**
- 5+ new versions each year
- Active Variants - Kitsune, Alpha, Beta, Canary

Frida | Instrumentation Tool

- Dynamic analysis & manipulation
- Function hooking
- Powerful debugging
- Evasion

Active Community

- **42 Contributors**
- Pre-written scripts & modules
- Updates twice a month



PCI Security Standards Council

Malware Evolution and Sophistication

Evolving Threat Landscape

Intercept MFA tokens

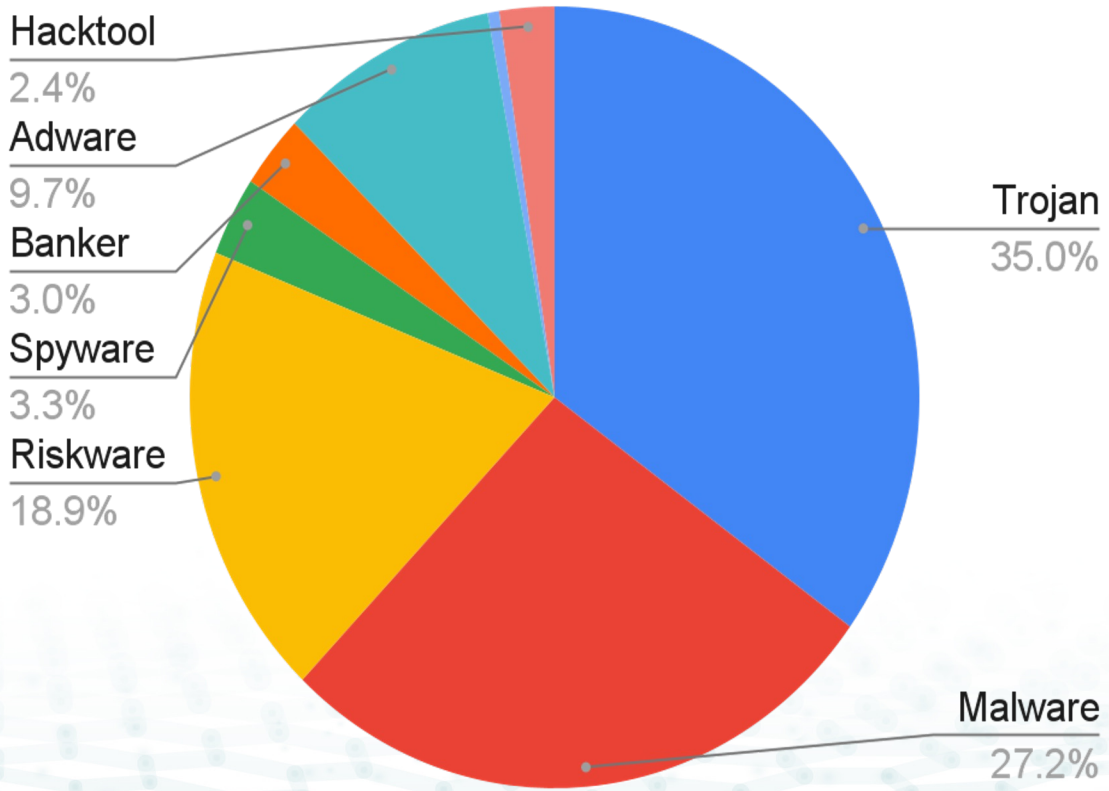
Disable Anti-Malware Apps

Detect & Evade Emulators

Abuse Accessibility Services

Screen Overlay Attacks

Real Time Screen Sharing



PCI Security Standards Council

Platform Vulnerabilities & Exploits

Evolving Threat Landscape

During 2022, **53%** of the Android devices detected as **compromised** were in the hands of attackers and **not just rooted** by users.

In 2023, a total of **943 CVEs** were reported for the Android operating system, a **45% increase since 2021**.

In 2023 there were **97 zero-day vulnerabilities** being exploited, a **50%** increase over last year.

PCI Security Standards Council

30+ Payments Customers

What Are Some Lesson Learned

PCI Security Standards Council

Challenges with Traditional Solutions

Lessons Learned

Static Protections Provides Limited Coverage

Inability to keep up with evolving reversing and tampering tools.

No ability to attest the device on-demand

Inability to assess device risk posture at any given time post-deployment

Lack of Threat Visibility

Inability to alert on attacks and keep up with new threats post-deployment

Security Best Practices

Lessons Learned

Need Multi-Layered App Hardening

Runtime security for Continuous Monitoring and Attestation

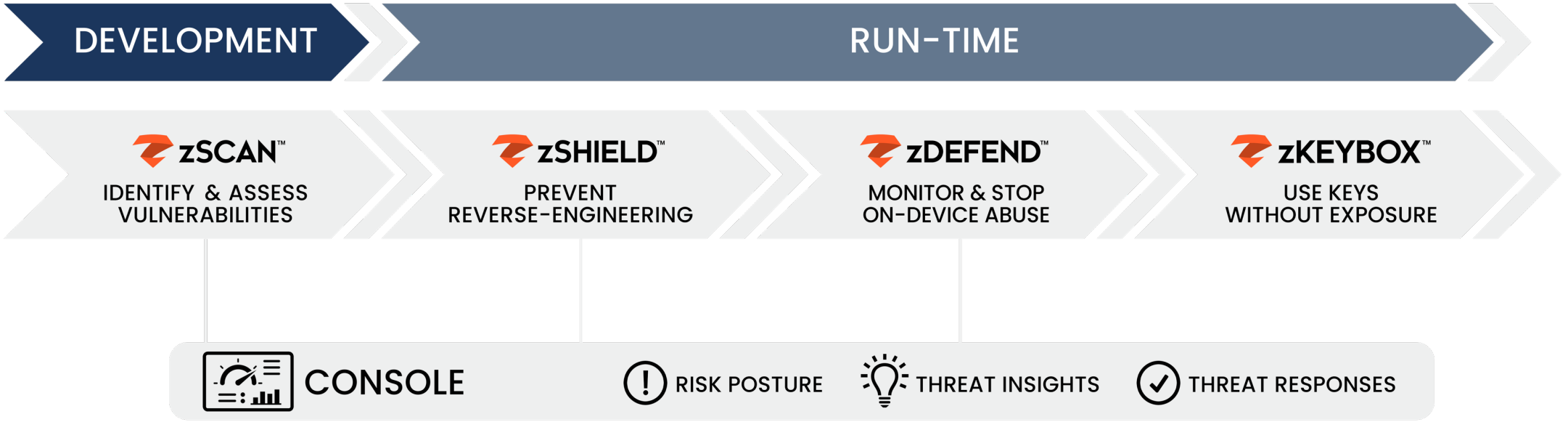
ML-Driven threat detection for “Zero-Day” protection

Leverage hardware-agnostic cryptographic keys & PIN protection

PCI Security Standards Council®

A Single Mobile App Security Platform

MAPS™



PCI Security Standards Council®

PCI Security Standards Council

Questions?

Stop by **Booth #9** during networking breaks

Thank You