SECURITY DEBT: WHAT LURKS BENEATH

Dave Lewis
Global Security Advocate
Akamai Technologies
@gattaca
WHOAMI

Dave Lewis
@gattaca
dave@akamai.com
Learning Objectives

1: Review what are you doing to address security debt.
2: Have you assessed the risk of security debt to your environment?
3: Quantify the expected financial loss due to an security debt outage.
Guardian Cloud Architecture
Guardian Cloud Architecture
Defining Security Debt
How Did We Get Here?

- Risk
  - Avoid
  - Accept
  - Reduce
  - Transfer
“Accepted The Risk”
Compound Interest

- Risks left unaddressed
- Years pass
- More software is added to the mix
- Layers of risk
- Danger grows with time and inaction
How IoT Drives The Cost Higher
The Fall Out

Unique IPs in the Mirai Botnet by day

- **First major Mirai attacks**
  - Unique IP Count: 2515727
  - Date: 9/22/2016

- **Attacks on Deutsche Telekom**
  - Unique IP Count: 2944317
  - Date: 11/27/2016

- **Satori variant modified**
  - Unique IP Count: 896181
  - Date: 11/29/2017
How Debt Can Grow
Ride The Cycle

- Identify
- Protect
- Detect
- Respond
The Flaming Sword of Justice!
Zero Trust
Security as Part of Mission

- Developers need to see security as a core competency of their skill set and mission
- All stakeholders need to be a part of the solution!
Bailing Wire & Duct Tape
Strategy as Defense
Trust But (Test) & Verify

- Trust the users...but, verify.
- Sanitize your inputs
- Sanitize your outputs
- Patch Patch PATCH
War Stories, So Many Stories...
Wrapping up...
THANK YOU