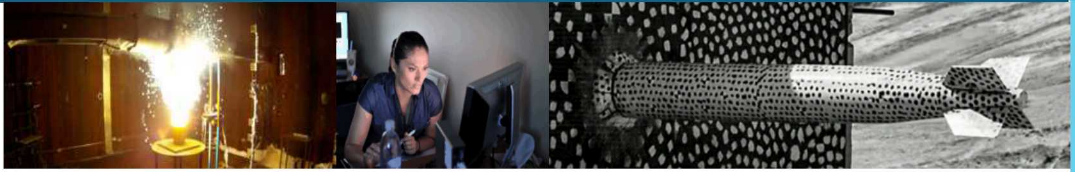
SAND2019-5441C

Using Awareness and Training to Enable Secure Software Development at Sandia National Laboratories



PRESENTED BY

Angela Rivas | acrivas@sandia.gov

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Software Security at Sandia

Mission:

Secure software, from the start.

Vision:

We build highly adaptive, self-securing, cyber resilient software and data systems.

Establish a Software Security Group (SSG)

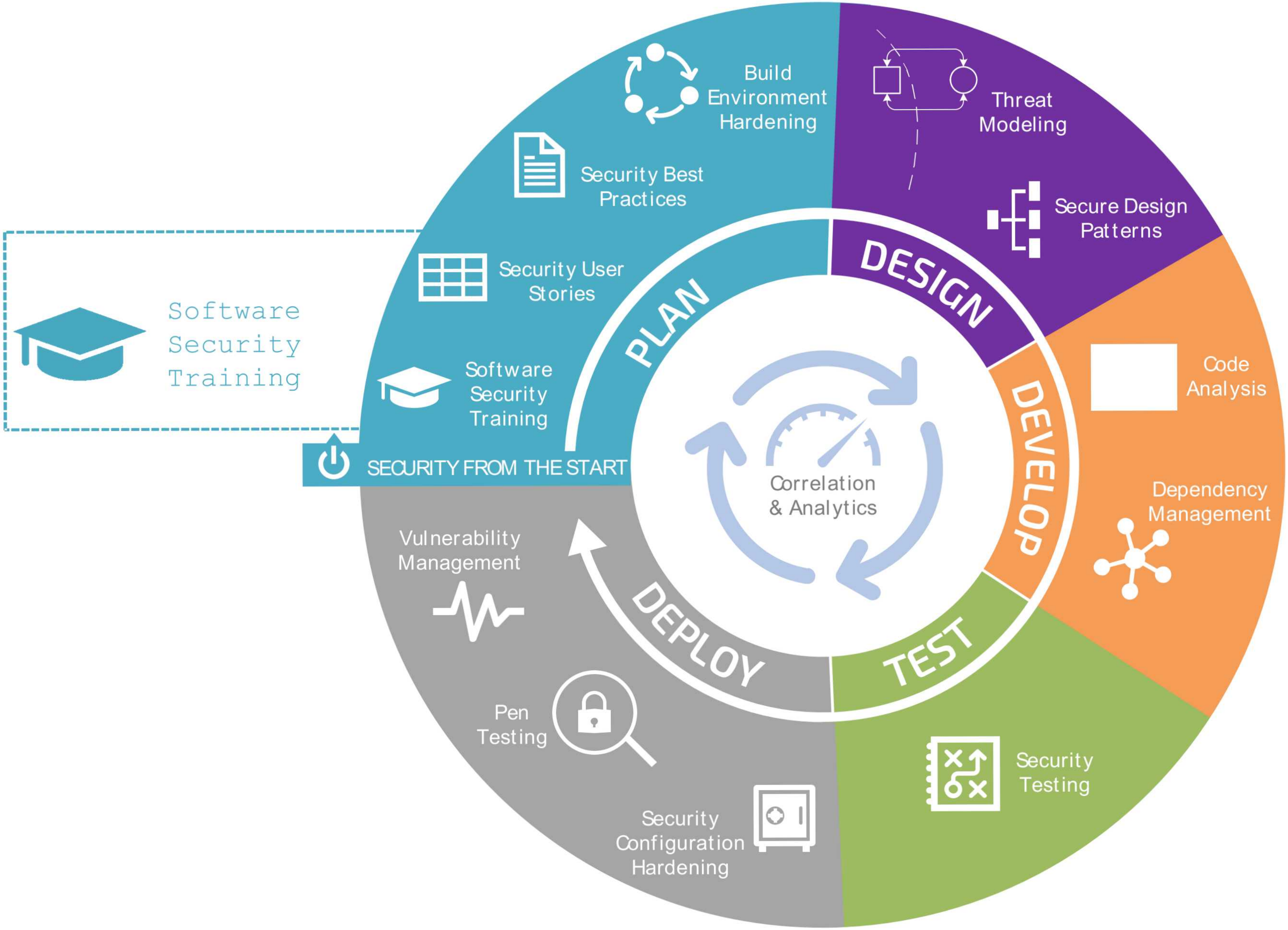
Enable a culture of secure software development

Provide enterprise services.

Build a program to develop technologies and methods to secure data and software from cyber-attacks

Establish and advance the Sandia strategy for data and software security

Security from the Start



Training is Needed

Cohesive, enterprise-wide training on how to develop secure software identified as an industry best practice in the 2017 Building Security In Maturity Model (BSIMM)

BSIMM

VERACODE

2017 study by Veracode: 68% of software developers say their organizations do not provide adequate training on application security.

Training is an Investment

> …we should be spending money on security training for developers. These are people who can be taught expertise in a fast-changing environment, and this is a situation where raising the average behavior increases the security of the overall system.
>
> **Bruce Schneier** - Writer, cryptographer

Awareness and Training

We provide:

- Awareness and tech
- Knowledge sharing
- Access to resources

so that every member of t development team underst security is his or her respo

Empower Software Developers

Software Security Awareness Training

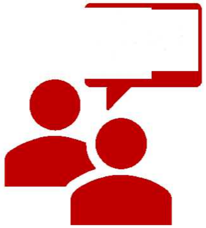
Developer Technical Training

Developer Secure Software Development Lifecycle (SDLC) Training and Application

Developer Deep Dive Dialogues

Software Security Awareness Training

For the entire software development team



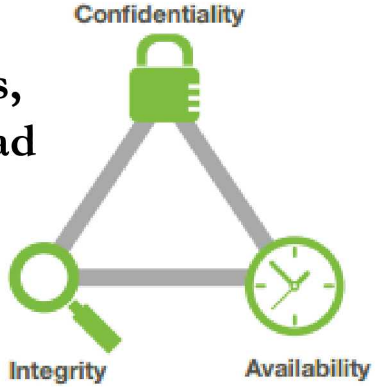
Awareness of the Problem

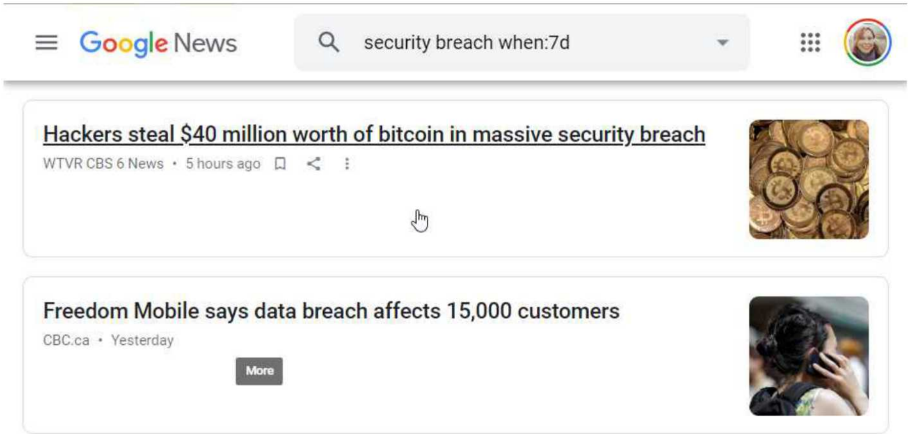
Awareness of the Solution

Key Outcome:
Understanding that there is a software security problem that affects us all but there are ways to eliminate or mitigate the threat of software vulnerabilities.

Awareness of the Problem

Security concepts, including CIA triad





security breach when:7d

Hackers steal $40 million worth of bitcoin in massive security breach

WTVR CBS 6 News • 5 hours ago

Freedom Mobile says data breach affects 15,000 customers

CBC.ca • Yesterday

Data breaches

Software Update Supply Chain Attacks: What You Need to Know

Software update supply chain attacks have been one of the big trends in cyber crime in 2018. Find out more about this cyber attack technique.

Security Response Follow
Oct 17, 2018 · 5 min read

Never miss a story from **Threat Intel**, when you sign up for Medium. Learn more

Supply chain risk

OWASP
Open Web Application
Security Project

Vulnerabilities, Juice Shop demos

Awareness of the Solution

1. Secure by Design
2. Model Threats
3. Validate Input
4. Sanitize data sent to other systems
5. Use canonicalization / normalization
6. Keep it Simple
7. Manage Risk in Third-party Components
8. Default Deny
9. Adhere to Least Privilege
10. Anticipate Errors
11. Secure the Development Toolchain
12. Use Static Analysis Security Testing Tools (SAST)
13. Use Dynamic Analysis Security Testing Tools (DAST)
14. Basic Quality Assurance
15. Practice defense in depth

Developer Technical Training

For developers

CHECKMARX

Codebashing

HUNTER2

SECURE CODE WARRIOR

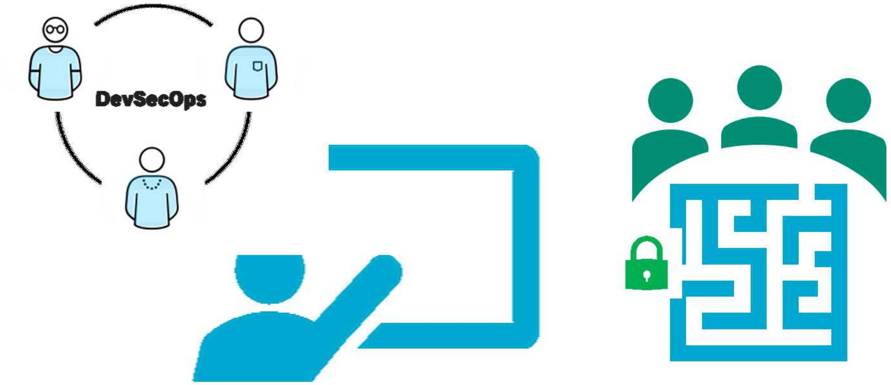
Placeholder for Coram's title slide (wiki is still down)

Interactive, hands-on training (COTS and in-house)

Key Outcome:
Learning more in-depth about vulnerabilities and mitigations, relevant to a particular framework or language.

Developer Secure Software Development Lifecycle (SDLC) Training and Application

For developers



Instructor-led lecture and labs with expert consulting

Key Outcome:
Gaining a holistic view of software security throughout the agile SDL and then applying security principles throughout their own projects.

Developer Deep Dive Dialogues

For developers

Curated content (videos, articles, books)

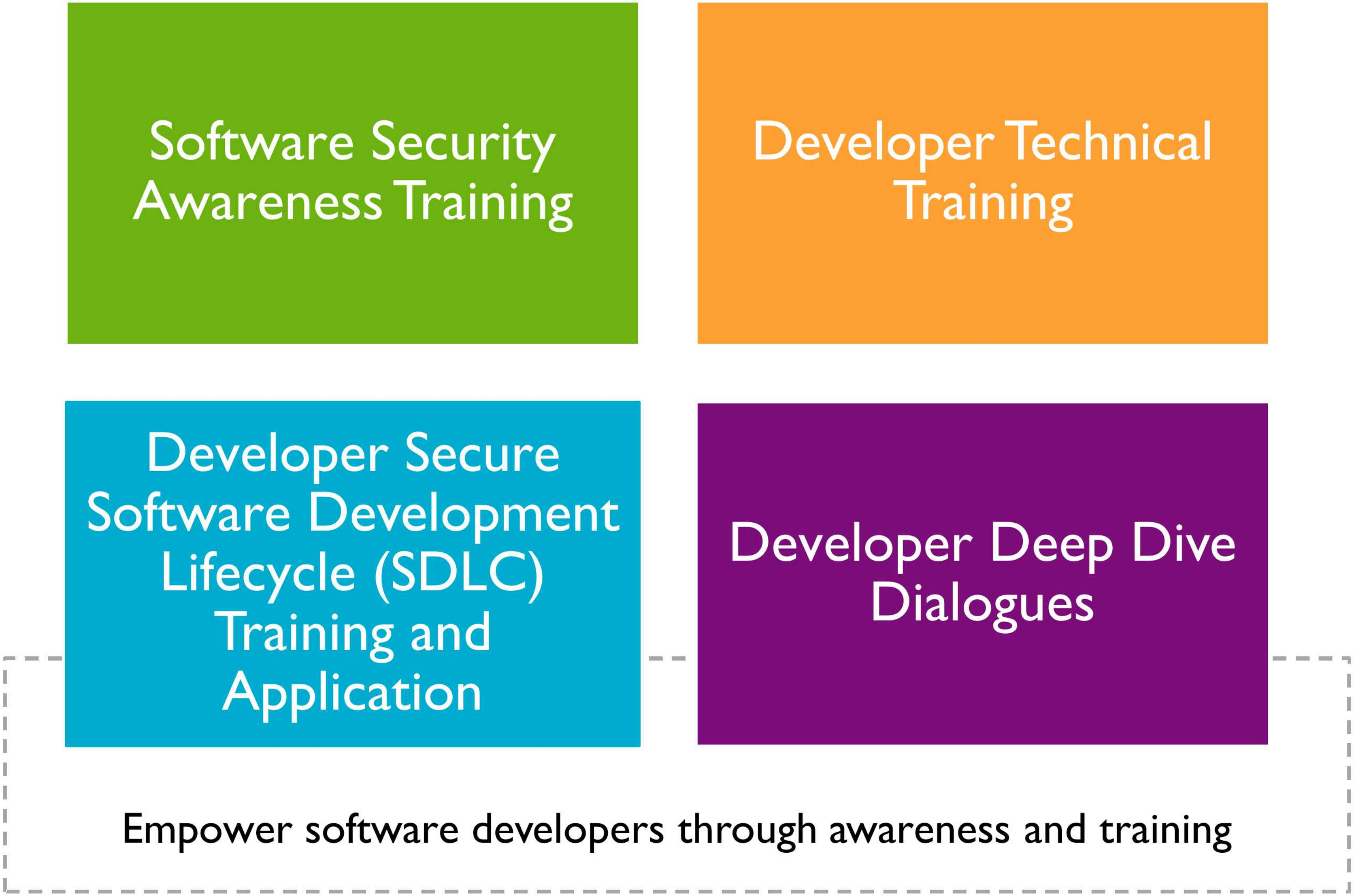
Facilitated discussion on a key software security topic

Key Outcome:
Enabling knowledge sharing by being able to learn with peers and inform each other about security practices across the laboratory.

Training Enables Security to Shift Left

> "…we also need to train developers, at the very earliest stage of their education, to bake security into all new code. It's not good enough to tack cybersecurity on as an afterthought anymore."
>
> **Carson Sweet** – CEO, Cloudpassage

Questions?



Software Security Awareness Training

Developer Technical Training

Developer Secure Software Development Lifecycle (SDLC) Training and Application

Developer Deep Dive Dialogues

Empower software developers through awareness and training

Learn more at NLIT!

Designing Security into Software Systems using Threat Modeling
10:00 AM - 10:40 AM : Room 120A
Gary Huang

Cross-Site Request Forgery Challenges and Solutions
10:45 AM - 11:25 AM : Room 110B
Michael Coram

Choosing Static Application Security Testing Tools
10:45 AM - 11:25 PM : Room 110B
Dr. Roger Hartley

Using Awareness and Training to Enable Secure Software Development at Sandia National Laboratories
10:00 AM - 10:40 AM : Room 120C
Angela Rivas

Benchmarking DevSecOps using Enterprise Search at Sandia National Laboratories
9:15 AM - 10:00 AM : Room 120A
Laritza Saenz