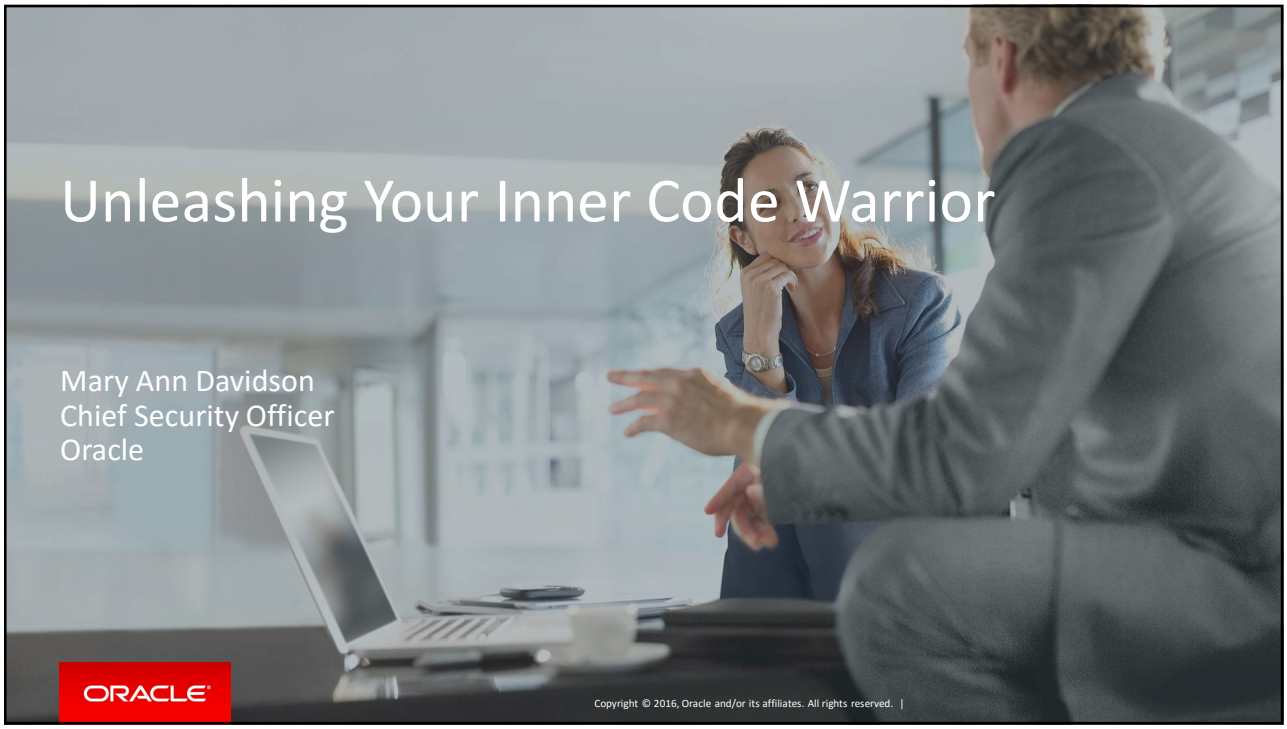


Why "Code Warrior?"

- The military has a lot to teach us about security – and leadership
- You can't win a war if you don't think you are in one
- "Warrior ethos" has prevailed over time
  - "Sid sibi pacem para bellum" – Juvenal
  - "He who defends everything defends nothing" – Frederick the Great
  - "Every Marine a rifleman" – US Marine Corps
- The military studies battles, trains for war, and does long-term defense planning – because there is *always* another war
- *Individual* warriors have changed history (not just generals!)
  - COL Pete Ellis, LCDR Wade McClusky

ORACLE

How Did We Get Here?

- Increasing IT backbone for ... almost everything
  - IP-enabled refrigerators...really?
- We have to relearn the same lessons with each technical rev
  - Rule 1 in secure coding...
  - Rule 2 (see Rule 1)
- Lack of a defensive mindset – because we don't teach this stuff!
  - "The University Story"
- Failure to collude constructively (and yet, the bad guys collude nicely!)
- Thinking of security as an "add-on" ... like rebar?
- We have a cultural problem

ORACLE

 3

So, What Do We Do?

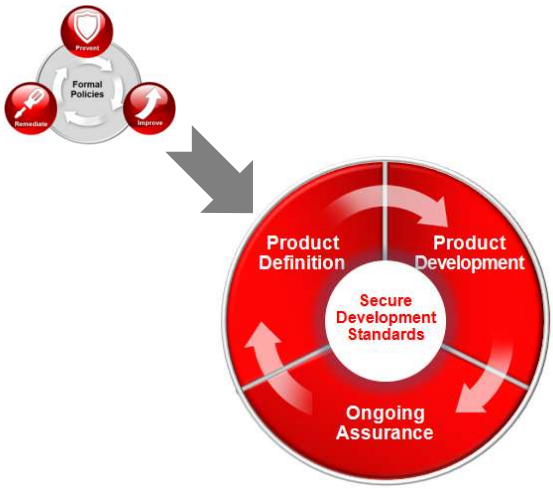
- Create a *culture* of security
  - Not just "secure code" - *way* more than that!
  - Organize, train, drill, measure, innovate, "red team/blue team" ...
  - "Boots on the ground" – not just "special forces"
  - *Continuously* embed and improve security
- Story: "The Little Dutch Boy"

ORACLE

 4

A Corporate Culture… Not Solely a Development Culture

- Formal policies and standards need to promote security culture
- Security culture cannot be limited solely to development
  - Impacts product documentation, support, patching, etc.
- Security focus cannot be limited solely to coding concerns (writing secure code)
  - Security must remain a concern throughout the product lifecycle



ORACLE

 5

What is Oracle Software Security Assurance?

… all the continuously improving processes, procedures, and technologies implemented by Oracle to ensure that Oracle's products and cloud services are meeting our customers' security requirements, while providing for the most cost-effective ownership experience.

ORACLE

 6

How's That Again?

- OSSA is designed to ensure that *whatever* Oracle delivers to customers (products, cloud services, consulting projects, etc.) has security embedded from development to delivery and throughout the product lifecycle

ORACLE

 7

How's That Again?

- OSSA encompasses
  - Security leads and security points of contact
  - Threat modeling
  - Secure design
  - Secure coding standards
  - Security education
  - Ethical hacking
  - Tools usage
  - Vulnerability handling
  - Secure by default
  - Compliance reporting

ORACLE

 8

Threat Modeling

- Architectural Risk Analysis requirements teach development teams how to analyze the threats faced ...
- ...and gives them a framework to build and improve their capabilities
- Feeds into better:
  - Design Documentation
  - Secure Configuration (Secure by Default)
  - Dynamic Analysis

ORACLE

 9

Secure Coding Standards

- First published in 1995, the Secure Coding Standards includes hundreds of directives and pages of guidance covering all aspects of secure coding:
  - Focused on the key issues that impact Oracle products
  - Backed by live, recorded and video training
  - Assessed by static analysis tools, both general purpose and SCS-specific
- The Oracle Secure Coding Standards now incorporate and adapt the CERT Secure Coding Standards
- The Secure Coding Standards are supported by additional informal coding guidance
- ...and are iterating to cloud

ORACLE

 10

Security Education

- All development staff must take a mandatory security education course:
  - Completion of this course is closely tracked
- Oracle hosts a wide range of on-line, on-demand training as well as regular live webcasts and hands-on classes for developers
- Specific training paths are suggested for different development roles

Ethical Hacking

- Ethical Hacking Team (EHT) performs security assessments of selected Oracle products
- The EHT use the types of attacks and analysis used by both criminal adversaries, customers' security teams, and IT security consultants
- The results of an assessment are used to improve the resources available to product development, e.g., the OSSA standards
- Assessments will also find vulnerabilities in the product and the EHT create product-specific recommendations to assist the development team in future

Tools Usage

- Oracle has made a significant investment in static code analysis
  - Early adopter of Fortify (2005); site license for Fortify since 2009
  - Oracle has developed an in-house general purpose static analyzer (Parfait)
  - Extensive guidance and training on how to configure, interpret and use static analysis reports
- Wide usage of commercial dynamic analysis tools
- Also specialized fuzz tools, focusing on Java, PL/SQL and Solaris among others (many developed by Ethical Hacking Team)
- Results fed into Oracle bug database, and are scored and triaged

ORACLE

 13

Vulnerability Handling

- Most security bugs are discovered internally (>80%) via OSSA and related activities
- They are fixed primarily in the main code line
- They may be backported through the Critical Patch Update program
  - Decision based on severity, likelihood of external detection, “patchability”, etc.
- Customers report the majority of externally discovered vulnerabilities
  - Customers get detailed status report about the bugs they have reported. They may also get early patches for testing purposes.
- Security researchers report small portion of vulnerabilities
  - However, greater portion in certain products (Java SE)
  - Security researchers get detailed status report about the bug they have reported and are notified when the bug is fixed.
  - Security researchers get public recognition in the credit section of the Critical Patch Update advisory

ORACLE

 14

Secure By Default

- Oracle products should install, by default, into a secure state:
  - Avoid default passwords
  - Use secure cryptography and communications protocols
  - Default to restrictive access control
  - Run at the lowest privileges possible
  - Minimize the attack surface
- Oracle's user documentation should also include detailed Security Guides:
  - Allowing customers to tailor the security configuration to their needs
  - Allowing developers to extend the product or build on the platform securely

ORACLE

 15

Release Security Checklist

- All teams must complete a security checklist before release
  - Checklist includes milestones at each phase of the development lifecycle
- The checklist assesses compliance with each OSSA standard
- Reviewed by the security management in each development team:
  - To carefully assess the level of compliance
  - To drive improvements in security processes and procedures
- Audited separately:
  - To improve the OSSA standards by giving more guidance and training where teams are struggling and spreading best practice and innovation
  - To identify potential "problem children" products and development teams

ORACLE

 16

Measuring OSSA Compliance

- Security Scorecard
  - Reports on security compliance of a number of critical products and services
    - Top five products by revenue
    - Strategic technology
    - Products on a security cure plan
  - Compliance reported to Oracle Security Oversight Committee and CEO
- Release tracking - OSSA compliance
  - Release security checklist (RSC) provides product and release level tracking of OSSA compliance for every product
  - Reviewed by development management and audited
  - Trend reporting across products within organizations is under development

ORACLE

 17

The Cost of Non-Compliance

- Vulnerability patching is much more expensive than vulnerability avoidance
  - Some patches have cost Oracle more than $1M for a single vulnerability to develop, test and distribute
  - Additional costs created for Legal, Public Relations, and other Corporate groups for highly visible problems
  - Reputational damage and lost sales are hard to quantify but clearly occur
- Increasing regulatory oversight of security adds to costs for noncompliance
  - Responding to regulatory action is very expensive in terms of executive, product development, and legal time
  - Possible penalties and other sanctions
- Graduated responses for internal non-compliance ranging from simple warning to cure plan and formal executive reporting

ORACLE

 18

A Few Stories

- "Houston, we have a problem…"
  - Moral: Try to resolve issues at the lowest level but don't be afraid to escalate.
- "With all due respect, sir…"
  - Moral: Support the troops.
- "16 days to do a build?"
  - Moral: It's not always about the technology.

ORACLE

 19

Takeaways

- "Let your yes be yes and your no be no."
- Whether you are George Patton or John Basilone, you can make a difference
- We cannot prevail without an innate *cultural* transformation around security – including understanding the limits of what we can protect

ORACLE

 20