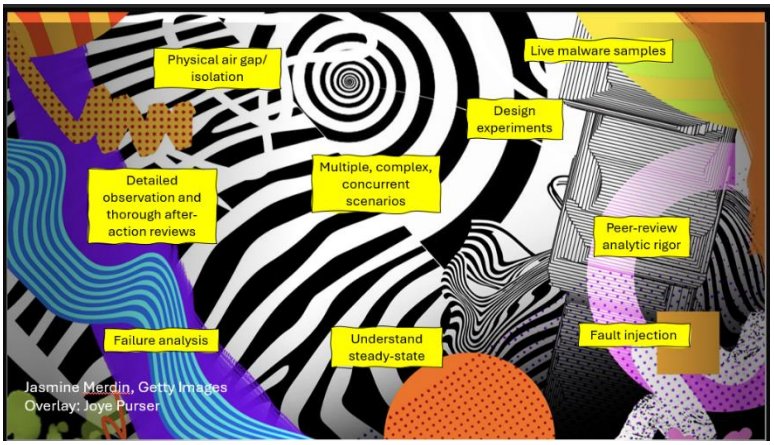
Secure Software, Inside and Out: Seven Steps

Joye Purser, CISSP, PhD; Jan Graves, CISSP; Walter Angerer

Joye.Purser@Veritas.com

Abstract

As a 40-year software industry veteran and 18-consecutive-year Gartner Magic Quadrant winner for data protection, Veritas Technologies constantly works to generate secure software. Leveraging CISA's "Secure by Design" principles for developers, Veritas incorporates people, processes, and technology to generate software products that are secure.



Incidents such as the SolarWinds attack presented an inflection point for Silicon Valley. The supply chain, or sequence of tools and activities employed to produce software products, has come under intense scrutiny. In this paper, we explain seven key phases of our SecDevOps process and how we employ chaos engineering to generate a robust product relied upon by 95% of global Fortune 100 companies.

In our discussion of 7 key steps in a mature SecDevOps process, we explain why chaos engineering techniques yield a better software product. Our Veritas REDLab is a unique, internal ‘cyber range’ where wild type malware is released into an isolated, test environment. This and other 'stress test' techniques harden our software during multiple points of the build process. True to our California roots, we build fun into the process and thus contribute to a positive company culture that retains talent and bolsters security.

Biography

Dr. Joye Purser is the Global Field CISO at Veritas Technologies. She consults with security leaders globally on all manner of cybersecurity topics. Before that, Dr. Purser served 18 years in the federal government in senior security executive roles, including the White House and Pentagon. She is the ISC2 Tipton Lifetime Achievement Award Winner for Information Security.

Jan Graves is the Chief Product Security Officer at Veritas. In this role he leads the organization responsible for the Application Security Assurance Program, product certification roadmaps, and oversees all aspects of secure software development. Prior to Veritas, Mr. Graves was Lead Systems Engineer for over a decade at Innovative Computer Systems, Inc.

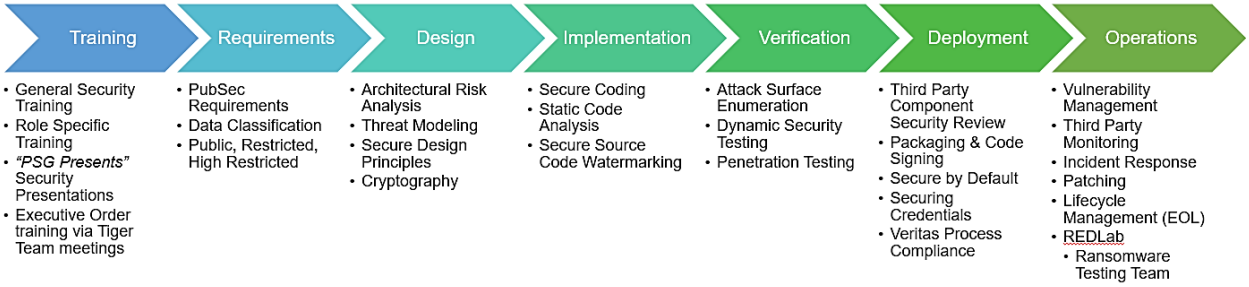
Walter Angerer is Senior Vice President of Engineering at Veritas and frequent public speaker on secure software development techniques. Before that, Mr. Angerer was CEO and Board Member of Parsec Labs, LLC, Quorum, and other data storage innovative startup companies. Earlier career experiences include software development and management at Siemens Power Transmission and Distribution.

1 Introduction

Software code developers have become modern day armor-makers. Cyber adversaries aggressively target code vulnerabilities. Both militaries and champion video gamers know that (a) knowledge of adversary vulnerabilities offers tactical advantage; and (b) defenders must know and understand their own vulnerabilities and aggressively control and protect such details among those with “need to know.”

Today’s software developers, teams, and leaders must concern themselves with much more than Agile processes. With cyber threat actors searching for any opportunity to exploit code vulnerabilities, the code itself must be developed securely. Robust information protection measures must be in place.

Thus, the concept of SecDevOps was born. This simply means that the processes by which software is coded and developed must include security at all stages. People, processes, and technology must align and work in close coordination to deliver “defense in depth” during the software development lifecycle: from design, code development, assembly, package, test, deploy and operation-and-maintenance (O&M). Teams are using chaos engineering techniques to test that code so it that is ‘hardened’ against the threat actors of today and tomorrow.



2 A Program for Application Security

The Veritas Application Security Assurance Program (ASAP) is based on Microsoft’s Secure Development Lifecycle for Agile Developers[1]. The program consists of seven, non-linear pillars. The pillars represent people, processes, and tools focused on a major phase *or* component of the software development lifecycle.

Over time, Veritas has evolved its methodology to address real-world challenges and requirements of *U.S. Presidential Executive Order 14028*[2]. When the Order was announced, we verified that we already followed the majority of the Secure Software Development Framework (SSDF) as outlined in NIST SP 800-218[3]. The Veritas Product Security Group (PSG) incorporates security practices throughout the entire development lifecycle for each software product. Veritas uses a variety of automated security tools as well as manual techniques to find vulnerabilities in our products in accordance with Executive Order and CISA requirements. Durable, dedicated teams meet with PSG bi-weekly on Application Security; Monthly on PubSec and Executive Order 14028 compliance.

2.1 Training

Veritas ensures that product development teams perform regular security awareness training to stay up to date with evolving security threats and mitigation techniques. Training also incorporates role-based scenarios to increase awareness of attack vectors and secure coding techniques. We incorporate chaos engineering techniques in our cyber-range awareness training: developers play the attacker’s role to better understand threats and mitigations under a variety of ever-changing scenarios.

2.2 Requirements and Compliance

A second pillar of our Application Security Assurance Program includes a program to track and monitor security and performance requirements. These requirements originate from our own internal standards, as well as regulations emanating from public sector and highly regulated customers such as financial organizations. Like a Governance, Risk, and Compliance (GRC) organization, our teams address the business case and cost implications of a large number of regulatory requirements. Our specialists evaluate that products follow secure design principles, such as least privilege, defense in depth, and secure defaults. They assess that software products have undergone threat modeling to identify potential security risks and vulnerabilities. They act as independent, internal auditors to monitor enforcement of Executive Order 14028 for items such as multi-factor authentication, encryption for data at rest and in transit (FIPS 140-2)[4], Zero Trust architecture, and software bill of materials (SBOMs). The teams also align best practices and security requirements with the SSDF.

2.3 Secure Software Design

Veritas works to ensure that secure design principles are met. Our Product Security Group assesses if each product has undergone threat modeling to identify potential security risks and vulnerabilities. Product teams follow “Secure by Design” principles defined by the Cybersecurity and Infrastructure Security Agency (CISA)[5]. At the tactical level, such principles include the use of memory safe program languages. A secure hardware foundation is employed, considering the hardware supply chain down to the chip level. Static and dynamic testing; code review by peers; defense-in-depth principles; and CISA Cyber Performance Goals are incorporated into our framework.

Products adhere to relevant security standards, regulations, and best practices; these include ISO 27001[6], the NIST Cybersecurity Framework, industry-specific security requirements

2.4 Implementation

The Implementation pillar includes processes to ensure product code reviews are conducted accurately and any issues identified have been addressed. Each product has undergone threat modeling to identify potential security risks and vulnerabilities. Products also have an extensive cryptography review as well as source code reviews, which seek to identify security flaws such as injection vulnerabilities, authentication bypass, or insecure data handling. We employ a control analysis tool is executed and that identified issues are addressed. Teams verify that the software product undergoes rigorous security testing. Teams address attack surface enumeration. We perform dynamic security testing and undergo penetration testing.

2.5 Deployment

This pillar validates that each product team enforces secure configuration management practices. We hire third parties to conduct independent Component Security Reviews. We conduct independent team oversight of packaging and code-signing processes. This includes securing credentials and ensuring overall process compliance. Related to vendors and third-party assessment: the PSG works with each product team to ensure that all vendors assess their third-party components and dependencies for potential security vulnerabilities or weaknesses. We enforce secure configuration management practices, such as storing credentials securely, protecting sensitive data, and implementing secure communication protocols.

2.6 Operations and Maintenance

In terms of product maintenance over time, we regularly assess and update our vulnerability policy for patching and other security-related code lifecycle management tasks. Veritas uses multiple automated security tools and manual techniques to find vulnerabilities in our products in accordance with Executive Order and CISA requirements. Veritas scores the severity of vulnerabilities using an industry standard system (Common Vulnerability Scoring System v3.1) to guide remediation urgency and public notifications. Dedicated product security leads meet with the Product Security Group bi-weekly to review application security topics. Veritas releases monthly security patches to ensure that customers have the latest fixes.

Product releases are not made available unless the PSG has approved a software bill of materials (SBOM). Veritas PSG generated a tool that uses heuristics to do basic validation of the SBOM delivered. The tool provides views of the data to simplify human review. The tool also identifies issues for reporting in the Plan of Action and Milestones. The product team and PSG review the tool results; human intervention is crucial in generating an SBOM. The SBOMs are delivered in machine-readable format, specifically, Software Package Data Exchange (SPDX)[7]. Veritas is exploring third-party validations for SBOMs and attestations for product compliance with the SSDF.

The Operations element validates that each product team has an established incident response plan, including procedures for handling security incidents, incident reporting, and communication channels.

3 REDLab

Veritas has also built REDLab[8], an isolated lab to study ransomware and malware attacks firsthand. we built Veritas REDLab, a proprietary, secure facility purpose-built to study the impact of live malware on our products. REDLab provides an isolated environment air-gapped from all Veritas network infrastructure. The lab uses live malware and ransomware variants to simulate real-world scenarios, testing our solutions to ensure it is hardened against modern threats at the technical level. We conduct our own research to study attacks as they occurred so we can (a) assess features to aid in detecting ransomware attacks; (b) improve protection of backup repositories; and (c) provide faster recovery when needed.

Staffed by senior security engineers from several established security organizations, REDLab is isolated from the outside world. Chaos engineering is employed to stress-test our software against a variety of adversary tactics, techniques, procedures (TTPs) and code variants. We have hired an external consulting team with more than 100 years of combined experience to validate our initial REDLab tests. These tests provided us with new insights into the inner workings of malware itself.

The REDLab initiative has improved our understanding of the requirements for infrastructure, applications, ransomware identification, and debugging. It also helped define how to simulate disaster recovery scenarios, as well as maintain, clean up, and quickly rebuild systems. The REDLab team synthesized learnings that contributed to ASAP improvements including: (a) implementing secure ways to bring in product binaries; (b) writing a product-specific fuzzer program to expose vulnerabilities; and (c) defining standard operating procedures to test and evaluation (T&E).

4 Conclusion

Signing the CISA Secure by Design Pledge is an important marker in a continuous evolution of our secure code development practice. Evolving our teams, skills, processes, and tools to meet tomorrow's software attacks is a high priority for us. Our ability to deliver data recovery in all-hazards scenarios is

paramount to our customers, and as critical IT infrastructure, we strive daily to produce software that is as clean, secure, and robust as possible.

It is our intent to share these practices with the broader developer community to build awareness and enhance our collective security.

5 Sources Cited

[1] Microsoft. “Microsoft Security Development Lifecycle (SDL).” Accessed September 11, 2024. https://www.microsoft.com/en-us/securityengineering/sdl.
[2] The White House. “Executive Order on Improving the Nation’s Cybersecurity, May 12, 2021.” Accessed September 11, 2024. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.
[3] NIST Computer Security Resource Center Special Publication 800-218. “Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities.” Accessed September 11, 2024. https://csrc.nist.gov/pubs/sp/800/218/final.
[4] NIST Computer Security Resource Center FIPS 140-2. “Security Requirements for Cryptographic Modules.” Accessed September 11, 2024. https://csrc.nist.gov/pubs/fips/140-2/upd2/final.
[5] CISA. “Secure by Design.” Accessed September 11, 2024. https://www.cisa.gov/securebydesign
[6] ISO, the International Organization for Standardization. “ISO/IEC 27001:2022, Information Security, Cybersecurity, and Privacy Protection — Information Security Management Systems Requirements.” Published Edition 3, 2022. Accessed September 11, 2024. https://www.iso.org/standard/27001.
[7] The Linux Foundation Projects. “System Package Data Exchange (SPDX®).” Accessed September 11, 2024. https://spdx.dev/.
[8] Veritas Technologies LLC. “Veritas Trust Center: REDLab.” Accessed September 11, 2024. https://www.veritas.com/why-veritas/trust/redlab.