Carbon Black.

Product Security Program

An overview of Carbon Black's Product Security Program and Practices

October 2017

Introduction

Carbon Black enables organizations to disrupt advanced attacks, deploy the best prevention strategies for their business, and leverage the expertise of 10,000 professionals to shift the balance of power to security teams. Only Carbon Black continuously records and centrally retains all endpoint activity, making it easy to track an attacker's every action, instantly scope every incident, unravel entire attacks and determine root causes. Carbon Black also offers a range of prevention options so organizations can match their endpoint defense to their business needs. Forward-thinking companies choose Carbon Black to arm their endpoints, enabling security teams to disrupt, defend and unite.

The security of our products is critical for our customers. We are committed to doing our part to secure our products..

The **Carbon Black Product Security Program** is a set of activities to secure our products through their lifecycle from planning to development and deployment. It includes three primary components:

- **Product Risk Management Plan**: a bottom up evaluation of the risks to product security, the mitigations in place to reduce risks and the areas we are investing to further reduce risks within our products.
- **Secure Development Lifecycle**: activities during software development required to ensure security is deliberately considered during planning, development and release testing.
- **Security Response Center**: monitoring for and responding to vulnerabilities in our products post-release.

This guide is an introduction to our Product Security Program, including an overview of these components and the activities contained within.

Product Risk Management Plan

The risk management plan defines why we invest in product security. It reviews the risks related to our products, mitigations in place to reduce those risks and the resulting residual risks. It aligns all stakeholders on the management plan for those risks. The resulting

security management philosophy is clearly communicated to engineering to enable wise implementation decisions. In an industry where customers rely on products to improve their own security posture, these are critical activities.

Development and management of the risk management process is a high-level and iterative approach, deeply integrated through the software development lifecycle. There are three goals:

- identify, rank, track and understand risks to product security
- identify operational activities in place to mitigate risks
- accept residual risks too low priority or too costly to mitigate

The Risk Management Plan is distinct from threat modeling or architecture reviews. Those activities are part of the Secure Development Lifecycle and apply the business's risk management philosophy to new development. They are executed by the development teams, derived from the guidance in the business's Risk Management Plan, and ensure consistency across product teams.

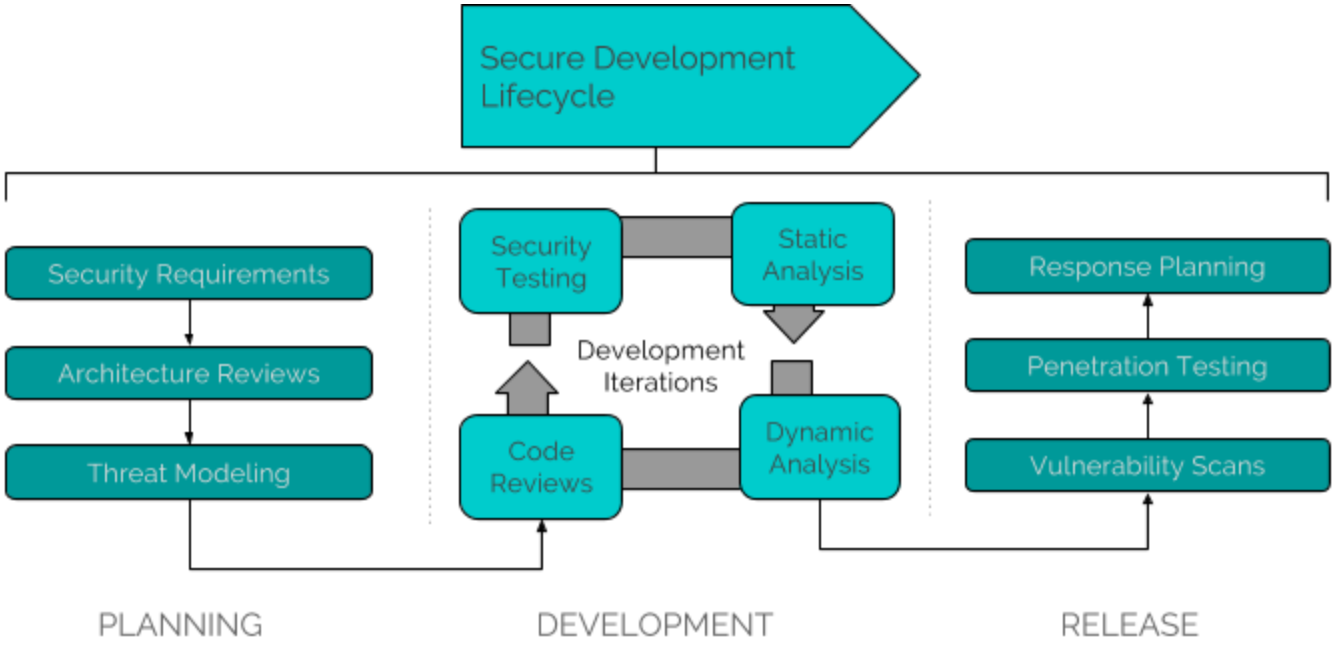
The product teams develop Carbon Black's Risk Management Plan with support from the product security group. The plan is renewed, reviewed and approved by Carbon Black's executive team every year.

Secure Development Lifecycle

Carbon Black's Secure Development Lifecycle (CB SDL) is designed to identify and mitigate product security risks during the product development phase. The CB SDL is heavily influenced by industry best practices such as Microsoft's Security Development Lifecycle, SAFECode (the Software Assurance Forum for Excellence in Code) and BSIMM (Building Security In Maturity Model). It is a collection of activities executed during the development process to ensure security during all development phases and include:

- Planning Phase
    - Security Requirement Review
    - Architecture Reviews
    - Threat Modeling
- Development Phase
    - Code Reviews
    - Static Analysis
    - Dynamic Analysis
    - API and UI Automated Scans
- Release

- External Vulnerability Scans
- Penetration Testing
- Security Response Planning and Coordination



The rigor of our process attempts to prevent vulnerabilities from deployment to customer sites and is evaluated regularly throughout the year to continue improving the security posture of our products.

Security Response Center

The Carbon Black Security Response Center (CB SRC) manages security vulnerabilities in Carbon Black products after release. The CB SRC receives product vulnerability reports from researchers, customers, partners, as well as through internal and third party testing. The CB SRC will validate the report, communicate to the reporter (if necessary) and queue the reported vulnerability for resolution. After each report is validated and remediated, CB SRC will communicate vulnerability details including severity, criticality, and any available workarounds and remediation procedures to customers via security advisories.

Our overarching goal as an organization is to ensure our customer's endpoint security is improved by the use of our products and any vulnerabilities which impact that goal are treated with urgency and transparency.

Appendix - Terms

Code Reviews - a systematic approach to peer-review all newly developed source code for mistakes. Security-sensitive areas require special reviews and approvals by security SMEs.

Dynamic Analysis - Source code analysis by a tool running code in a "sandbox" with detailed instrumentation to observe runtime behavior. Provides a richer understanding of code structure and flags potentially unsafe conditions for review.

Penetration Testing - In this case, application penetration testing, the focused testing of an application not to test the functionality, but to discover and exploit vulnerabilities. Assessments usually completed manually by humans who are subject matter experts, in contrast to vulnerability scans which use scanning tools to accomplish a similar goal.

Secure Development Lifecycle (SDL) - a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost.

Software Development Lifecycle (SDLC) - a framework defining tasks performed at each step in the software development process. SDLC is a structure followed by a development team within the software organization. It consists of a detailed plan describing how to develop, maintain and replace specific software.

Static Analysis - Source code analysis by a tool that to provide an understanding of code structure, ensure code adheres to industry standards and flag potentially unsafe conditions for review.

Threat Modeling - a structured approach that enables you to identify, quantify, and address the security risks associated with an application.

Vulnerability scanning - the use of automated tools to scan applications (typically web applications) to look for known security vulnerabilities such as cross-site scripting, SQL injection, command execution, directory traversal and insecure server configuration.