SECURITY COMPASS WHITEPAPER

Building a Product Security Practice in a DevOps World

Security Compass

Authors:

Eleonor Lee
Sr. Product Marketing Manager
Security Compass

Arun Prabhakar
Security Consultant
Security Compass

Altaz Valani
Director of Insights Research
Security Compass

There is much emphasis today on development and delivery. The narrative largely focuses on speed of software delivery through automated pipelines. Unfortunately, little attention has been paid to product security. However, product security is gaining popularity slowly.

One example is the recent introduction of CWE Hardware by MITRE.

With the integration of product and software lifecycle workflows, managing security across both domains is becoming an essential capability. This capability applies to many industry verticals including manufacturing (e.g. electronic, semiconductor and industrial manufacturing), IT software, and others. The key aspect is being able to integrate software and product life cycles in a coherent manner so that the final product release is secure. In this whitepaper, we will discuss key product security capabilities and a holistic governance framework to bring these two domains together without slowing down the business.

What differentiates product security from software security?

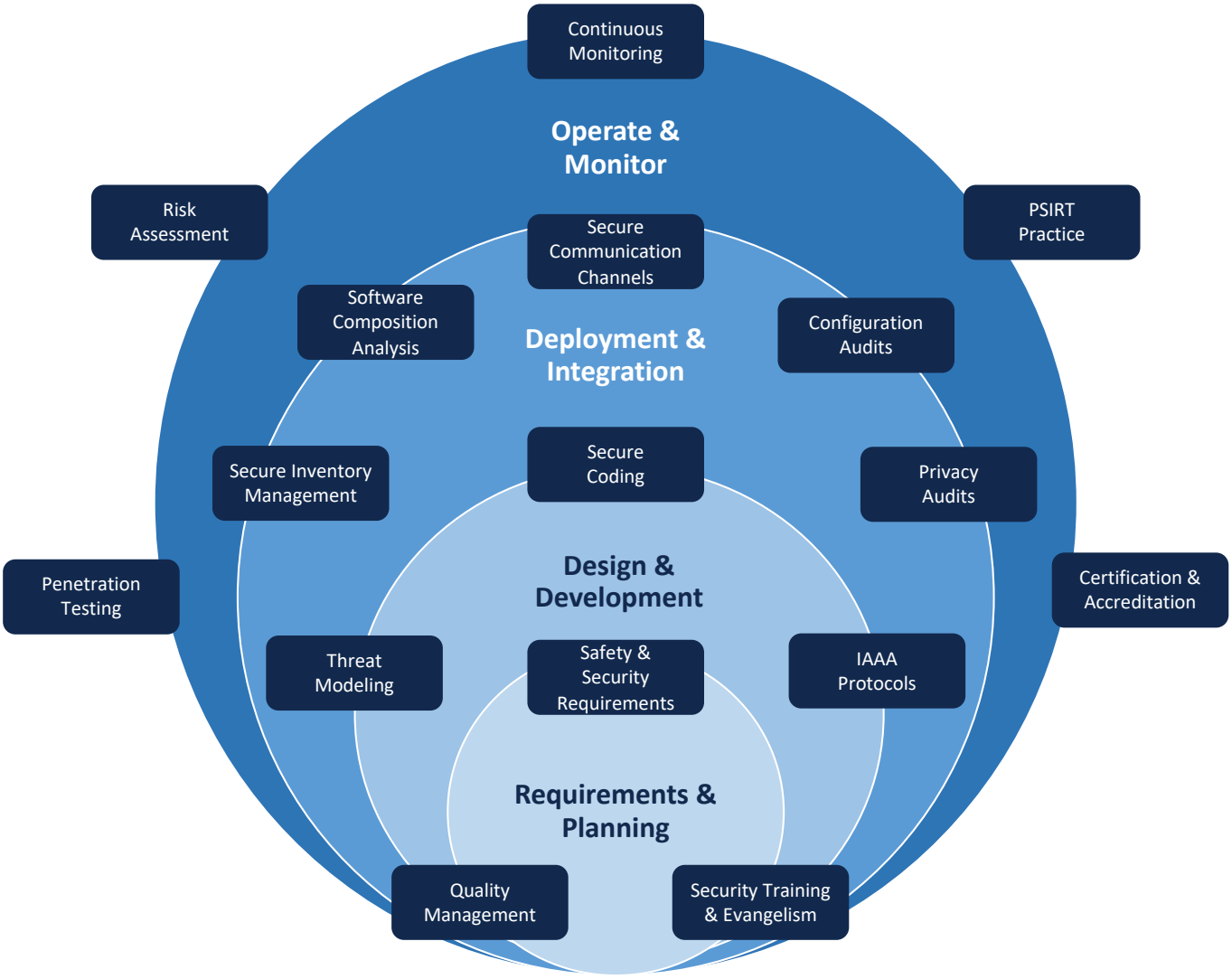
It is important to understand the key differences between software and product security. While both domains are trying to be secure, their constraints are different:

Software Security	Product Security
Can easily make changes after release	Changes can be difficult or impossible
Shelf life of software is a few years	Shelf life can be decades
Rich ecosystem of security automation	Few tools available for automation

Building key product security capabilities

The figure below is a snapshot of the different security capabilities that enterprises involved in product development should plan to establish and practice, in order to accomplish a better security risk posture throughout the lifecycle of the product. The services of the capabilities established must be leveraged in a phased manner right from the inception stage. To balance between the traditional and DevOps methodology, we have identified four phases for the product development lifecycle:

- Requirements and Planning
- Design and Development
- Deployment and Integration
- Operation and Monitoring.



Requirements & Planning

A. **Quality management:** One of the important elements that engineering teams must consider right from the initial phases is building a quality product. A quality product means everything including higher performance, greater reliability, lower operating cost and so on. Quality management systems are seen as a driving factor behind many of the verification and validation procedures that are carried out in the world of product security. There are many methodologies including Lean and Six Sigma which have the tools and techniques to help build quality products.

B. **Safety and security requirements:** Designing products, especially in the manufacturing sector, requires consideration for a lot of safety requirements as mandated by varied regulations and standards, pertinent to the domains and geography of the consumer using the product.

   One example is IEC 61508, an international functional safety standard which provides a framework for safety lifecycle activities. The standard covers safety-related systems which incorporate electrical/electronic/programmable electronic devices. Many of the failures in hardware and embedded devices may threaten human life safety and care must be taken by considering the hazard identification and damage limitation steps. This is in addition to considering **security requirements** that must be adhered to secure the complete product. A good reference to start with would be the ISA 62443 standard that specifies security capabilities for control system standards.

C. **Security training** plays a key role and must be done at every stage of product development to all stakeholders. Based on the role, domain and other aspects, the right training given at the right time will enable teams to build a secure product. There must be customized training rolled out on a mandatory basis to the teams involved and security professionals must play the role of evangelists, not just gatekeepers to sign off and perform assessments.

Design & Development

A. **Threat model:** The importance of **Secure Design** and **Threat Modeling** are well known to the professionals building software products. These activities in fact carry more weight in the world of product security. Some of the hardware security attributes like encryption methods, obfuscation techniques are critical secure design techniques implemented in devices and integrated circuits. There are many commercial Electronic Design Automation (EDA) tools that assist in the design and verification of secure hardware. Architects and security professionals must assess all the scenarios to evaluate the threats in the overall solution for which the product is designed for.

B. **IAAA protocols:** There is a plethora of devices, services, third-party components, that are integrated for product security. On top of that, many defensive layer security measures have to be planned and not all of them are in-built, coded, or configured. Organizations use many vendor solutions, secure libraries, and certified tools for establishing the Identity, Authentication, Authorization and Accountability **(IAAA Solutions).**

C. **Secure coding:** There are many teams at every layer that convert the security requirements captured into an actionable program by using the respective languages at those layers. For example, the use of VHDL (VHSIC Hardware Description Language) by the hardware teams while specifying the structure of a digital circuit, or when using embedded C language for programming microcontroller-based applications or the use of java when writing a software application. It is important that secure coding measures are incorporated during those times. This is a good place of reference for secure coding in embedded systems.

Deployment & Integration

A. **Secure communications:** We have called out this as a separate capability since product development is all about integrating many pieces together and it is essential to secure the communication of the complete stack. There are many communication channels, the device to device, the device to machine, machine to machine, within cloud, on-prem, etc. It is not going to be within the accountability of one team to take care of the end-to-end security. Hence this requires a careful planning by the admins of the Operations or SecOps team.

B. **Secure inventory management:** Having an inventory of authorized and unauthorized devices is an important security control in an environment operating with a lot of devices. In order to have an effective defense on the network we need to have an inventory of all the devices that are used. Going by the access control principles, only authorized devices must be allowed access and unauthorized, unmanaged, and unsupported devices must not be given access inside the network. The information will help further in collecting all the relevant attributes for the devices in the environment.

C. **Software composition analysis:** Business units that manage a large portfolio of products certainly need SCA tools. There is a lot of open source code being leveraged by software developers as they focus on rapid time to market. It is estimated that FOSS (Free and Open source) tools make up to 60 to 80 percent of application code base, hence managing risk has become a top priority. SCA tools not only help manage the inventory of such open source tools but also help in mitigating the security vulnerabilities.

D. **Configuration audits:** This is an important activity to perform for products that have a variety of devices built into it. Configuration audits, in general, validate the integrity of product configuration information. There are two critical parameters that should be of interest to product development teams, one is the Functional Configuration Audit (FCA) and the other is Physical Configuration Audit (PCA). FCA examines the functional characteristics of the configured product and verifies that the product has met the requirements specified whereas PCA examines the actual configuration of an item being produced.

E. **Privacy audits:** Though privacy assessments should be an implicit part of the security activities that are performed throughout the lifecycle of the product development, there is a lot of weightage given to privacy assessments these days by auditors and regulators. In the last few years, the industry has seen many data breaches impacting privacy, especially in the manufacturing industry. Based on the domain, geographical presence, and compliance, these privacy checks will vary. The International Association of Privacy Professionals owns a lot of resources with regards to privacy and has some good guidelines for professionals on privacy assessments.

Operate & Monitor

A. **PSIRT practice:** The first half of the last decade saw many security attacks on the transport layer security, BEAST, FREAK, POODLE, and a lot more. Every product team would have mandatorily addressed the security in transit during the pre-production stages, but attackers have found many ways to bypass those security controls during the production environment. SSL based issues are just an example, issues like these happen at every layer of the product. This is an ongoing threat and the enterprises must set up a Product Security Incident Response Team (PSIRT) that gets to know about the potential vulnerability in the products that could expose organizations and consumers to security risk. The PSIRT can then coordinate with the engineering team to identify an appropriate course of action.

B. **Continuous monitoring:** There are many products designed to safeguard human lives, that are deployed at coal mines, hospitals, construction sites, it is important to continuously monitor these systems for any data loss, malware intrusions that disturb the integrity and availability of the system. The regular software security solutions might not help in these circumstances. We need solutions that are designed to accommodate the protocols used in the related domains. For example, a regular firewall used for IT applications may be ineffective to protect SCADA solutions or automotive products running CAN protocols. The Security operations team running DLP, SOC practice must have the required resources and specialist to catch these issues.

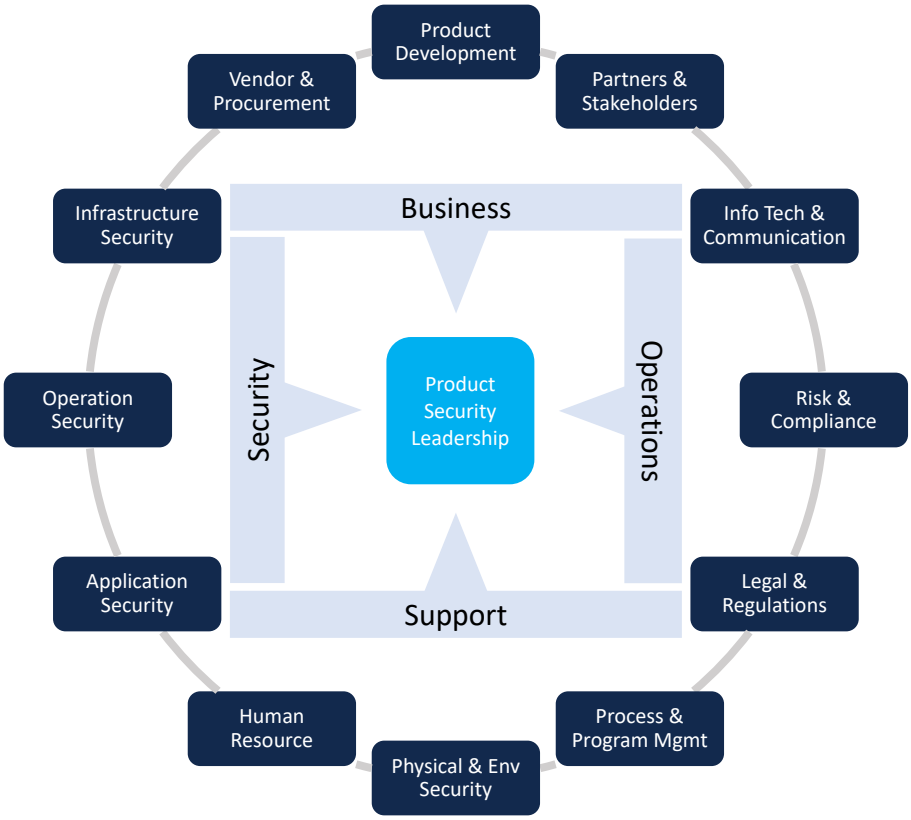
C. **Penetration Testing:** This is the last step in the Product Security process but be done periodically or when there is a need for it. It must be carried out by internal teams and also by trusted and certified vendors. Also, pentesting is a specialized process in product development scenarios. It is about crafting attack vectors that can exploit any layer, say the JTAG interfaces at the hardware level, the domain specific communication protocols like MODBUS or CAN, the vulnerabilities at the edge layer or the software operating in the cloud. There are special tools and certified professionals to perform these.

D. **Certification and Accreditation:** Certification is the technical evaluation of a system or product and its security components. Accreditation is management's formal approval and acceptance of the security provided by a system. When an enterprise plans to launch a product, there is a clear mandate from the government to follow security standards and achieve the required certifications. Some of the common certifications that product vendors go through involve the common criteria that assesses the effectiveness of the security controls built into a system from functional and assurance perspectives or the FIPS 140-2 which is the cryptographic validation standard. There are many service providers that help with the complete certification lifecycle.

E. Risk Assessment: Risk Assessment is the activity that conveys to the business the technical impact of security into a language that business professionals need. In addition to identifying assets, threats and vulnerabilities, risk analysis focuses on the impact that the controls have on the cost and benefits to the overall organization. There are many methods that will help in the Risk Analysis process but it is important to quantify the risk so that business has the insights on Exposure Factor, Annualized Rate of Occurrence, etc. From a product security perspective, the international standard ISO 10377:2013 (Consumer product safety – Guidelines for suppliers), includes guidance for suppliers about product risk assessment and considers safety in design, production and in the marketplace. This is a critical activity that must be performed for the overall risk management or for activities like Business Continuity Management.

Governance of product security

At a strategic level, governance implies the creation of competencies that are essential to delivering a secure product. Within that context, here are the key competencies:



At the operational level, we need to identify the roles, processes, and controls. Each role has a part to play in the overall value delivery process for software and hardware components. The security controls are there to ensure that risk against an acceptable threshold is being met. This can be, for example, in the form of compliance to software and/or hardware standards or frameworks.

	Functions	Roles	Responsibilities	Accountability
Business	Product Development & Management	Architects, Developers, Testers, Domain Experts Product Manager Business Analyst	Work on the business requirements to develop a fully functioning product that is reliable and resilient so that it meets quality constraints and consumers expectations. Responsible for ROI, market opportunities and feature differentiation	a) Manage security throughout product lifecycle b) Adhere to DevSecOps practices c) Manage Revenue, Gross margin, Time to market
	Partners & Stakeholders	Investors, Customers, Government Authorities, Researchers	Sponsoring the product development, providing constant feedback, and helping build secure but profitable model and validating the shippable increments	a) Assure end-to-end financial support throughout lifecycle b) Provide required assistance to address complex security challenges
	Vendor & Procurement	Suppliers & Distributors Service Providers Procurement Leads	Timely availability of relevant resources by purchasing or through acquisitions, capturing the secure requirements in contractual agreements and licensing terms.	a) Thoroughly monitoring the SLA to maintain business continuity b) Researching to partner with vendors that provide quality products/service
Operations	Information Tech & Communication	System Administrators Hardware Technician Network Engineer Integrations Manager	Set up, install and maintain security tools across all products, monitor and configure systems based on the policy requirements, approve and determine device management	a) Qualify system behavior based on Acceptable usage policy b) Maintain secure practices in packaging & deploying products
	Risk & Compliance	Compliance Managers, IS Auditors Risk Officers	Ensure compliance to standards, best practices, policies, perform periodic audits in every aspect of the product and assess risk at every level and across the product teams	a) Mandate compliance checks at every stage of product lifecycle b) Mitigate, manage risk with every department of product development
	Legal & Regulatory	Corporate Counsel Legal Secretary Regulatory Specialists	Administer and standardize overall business operations with respect to regulatory aspects by assessing policies and risk. Being prepared for legal ramifications and subsequent actions.	a) Monitor due diligence in legal matters involved with all stakeholders b) Ensure periodic audits cover the applicable regulations

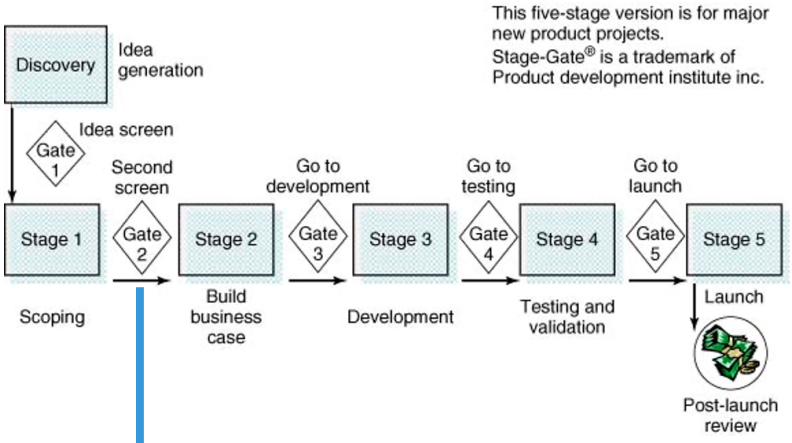
	Functions	Roles	Responsibilities	Accountability
Support	Process & Program Management	Scrum Masters Program Managers Quality Management Champions	Practice the culture of continuous process improvement, mentor and monitor quality. Enable collaboration among teams, practice secure SDLC and DevSecOps process	a) Prioritizing security requirements in every release and sprint b) Foresee blockers such that teams don't see cost and time issues in applying security controls
	Physical & Environment Security	Facility Managers Business Continuity Experts Emergency Response Teams (ERT) Specialists	Being prepared for a product failure and ensure continuity in the ongoing operations. Manages recovery solutions and implements redundant methods to keep damage under control	a) Preparedness for human life safety measures in the event of product failure. b) Perform audits that checks the physical access made to the product
	Human Resource	HR Representatives Staffing specialists Training Specialists	Hiring the right talent for different teams and performing background checks. Taking measures for personnel safety. Developing awareness campaign on security practices.	a) Mandate relevant security trainings for all stakeholders. b) Prioritizing personnel safety while partnering with business units
Security	Application Security	Threat Modelers AppSec Engineer Cryptanalysts	Perform threat and vulnerability management across software and hardware application. Mitigating the security risk by applying and configuring defensive coding practices	a) Perform comprehensive analysis of application throughout lifecycle b) Timely remediation of vulnerabilities and flaws to minimize the overall risk
	Operation Security	SOC Analysts Firewall Admins Forensics Analyst Data Loss Professionals	Responsible for the ongoing support and acts as the first line of defense. Takes every attempt to detect a compromise underway and alert admins/ take appropriate actions.	a) Prioritizing security and risk in trade-off decisions (cost, performance, etc) b) Taking prompt response to avoid and control damage
	Infrastructure Security	Network Security Admin Pentesters Cloud Security Architect IOT Security Specialist	Responsible for deployment and platform security and provide security assurance by black box testing methods	a) Validating every aspect before providing a final security sign off b) Developing vulnerability, patch and configuration management plan to roll-out to vendors and partners.

Integrating product development and secure software development life cycles

Employing a governance process that enables your product development lifecycle to go in tandem with secure software development lifecycle promotes cross-functional collaboration, efficiency and speed in bringing secure products to market. This entails leveraging the strengths of the secure development lifecycle framework and tools — particularly in managing requirements, secure development guidelines, test cases and test results, and integrating this with established product innovation and launch framework, such as the one shown below.

A secure development process overlaid at various stages of product development ensures security is built from the ground up in all aspects of their product — hardware, software and firmware — from initial design through to testing, deployment and ongoing monitoring. A tight integration between these processes becomes increasingly important as most hardware products also include an element of software and/or firmware to manage the device. Hardware products are also increasingly launched with additional feature and functionality updates, so that they can be more fluid and flexible in nature even after they have been deployed in the field.

Product Development Framework



Secure Development Framework

Requirements & Planning	Design & Development	Deployment & Integration	Operate & Monitor
Quality management	Threat model	Secure communications	PSIRT practice
Safety & security requirements	IAAA protocols	Secure inventory management	Continuous monitoring
Security training	Secure coding	Software composition analysis	Penetration testing analysis
		Coniguration audits	Certification & accreditation
		Privacy audits	Risk assessment

Source: Wiley Online Library

Conclusion

Product security is becoming more important as we see the convergence of software and hardware lifecycles. The challenge is trying to integrate the processes and tools in a way that is not disruptive to business speed, while remaining within risk thresholds for security and compliance. This implies collaboration across multiple stakeholders, with each stakeholder contributing to the balance between speed and risk.

Security Compass

Go Fast. Stay Safe.

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to adopt Balanced Development Automation for rapid and secure application development. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on howorganizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit them at securitycompass.com to learn more.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
600 California Street
San Francisco, California
USA 94108

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001