Product security strategy

The assignment is to build out and scale a product security program, ensuring that products are developed with security in mind.

In smaller organizations, this assignment will often be shared by the (C)ISO, in larger organizations this is most often covered by a separate role.

Examples of roles with this assignment:

- Product Security Officer
- Product Security Architect
- CISO

EU Cybersecurity Skills Framework: (Imperfect match) Chief Information Security Officer (CISO)

Security Skills

- High-level SDLC (Secure Development LifeCycle) knowledge
- Selecting and using security frameworks
- Risk assessment expertise

Security Training Resources

- OWASP SAMM (Deep dive – be able to explain the model in depth)
- BSIMM (BSIMM provides insight in practices at large companies)
- Peer groups such as the Let's Talk Software Security Meetup Group

Books

- Secure and Resilient Software Design (ISBN 9781498759618)
- Alice and Bob Learn Application Security (ISBN 9781119687405
- The Security Culture Playbook (ISBN 9781119875239)
- Software Security (ISBN 9780321356703)

Relevant Security Certifications

- Paul Jerimy's Certification roadmap, focus on broad mid-level and specialized high-level certifications in "Security and Risk Management" as well as "Software Security"
- ISC2 CSSLP (Certified Secure Software Lifecycle Professional)
- GIAC GSSP (GIAC Secure Software Programmer)

Organizational Security Strategy

The assignment is to oversee the organization's cybersecurity strategy and its effective implementation to ensure protection of systems, services, and assets.

This role will default to a CISO role in most organizations except for very large ones, where it might be found at the business unit level.

Examples of roles with this assignment:

- CISO
- BISO
- Security Officer

EU Cybersecurity Skills Framework: Chief Information Security Officer (CISO)

Security Skills

- Understanding of security policies
- Risk management expertise
- Regulatory & compliance knowledge

Security Training Resources

- Microsoft Chief Information Security Officer (CISO) Workshop Training
- OWASP SAMM
- NIST Cybersecurity Framework
- NIST Risk Management Framework
- SANS Security Policy Templates: Free templates

Books

- The Security Culture Playbook (ISBN 9781119875239)
- The CISO Evolution: Business Knowledge for Cybersecurity Executives (ISBN 9781119782483)

Relevant Security Certifications

- Paul Jerimy's Certification roadmap, domain "Security and Risk Management"
- ISC2 - CISSP (Certified Information Systems Security Professional)
- Various - ISO/IEC 27001 Lead Implementer

Business Strategy

The assignment is to set strategic direction, make high-level decisions, and lead different areas of the business to achieve the company's overall objectives.

This is the "rest of the C-suite" and is included in this list because of the importance of management buy-in, as well as the management assignment for security.

Examples of roles with this assignment:

- C-level executive
- Business unit manager
- VP

EU Cybersecurity Skills Framework: N/A

Security Skills

- Business acumen (Security can be an enabler/differentiator!)
- Risk management

Security Training Resources

- Harvard Online Course - Managing Risk in the Information Age
- C-Level Cybersecurity awareness courses (Various paid offerings are available, or courses can be built in-company)

Books

- Cybersecurity for Executives: A Practical Guide (ISBN 9781118908801)

Relevant Security Certifications

- ISACA – CGEIT (Certified in the Governance of Enterprise IT)
- SANS Institute – GSLC (GIAC Security Leadership Certification)

Architecture

The assignment is to oversee the overall structure of systems or projects, ensuring that technical solutions align with business objectives and requirements.

Security can be a specialization in (system) architecture, but most often it needs to be considered together with the other "ilities" by every architect.

Examples of roles with this assignment:

- Product Security Architect
- Architect
- Lead Developer

EU Cybersecurity Skills Framework: Cybersecurity Architect

Security Skills

- Security architecture
- Security standards
- Threat modeling

Security Training Resources

- NIST - Engineering Trustworthy Secure Systems
- SANS SEC530 - Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise
- Various applicable standards (ETSI / IEC / NIST..)
  eg. NIST SP800 series, IEC62443-4-2, ETSI 303645
- OWASP ASVS

Books

- Security Engineering: A Guide to Building Dependable Distributed Systems (ISBN 9780470068526)
- Threat Modeling: Designing for Security (ISBN 9781118809993)
- Threat Modeling: A Practical Guide for Development Teams (ISBN 9781492056553)

Relevant Security Certifications

- Paul Jerimy's Certification roadmap, domain "Security Architecture and Engineering"
- (ISC)² – CISSP-ISSAP (Information Systems Security Architecture Professional)
- TOGAF - Integrating Risk and Security within a TOGAF Enterprise Architecture
- SABSA - Chartered Security Architect – Foundation Certificate (SCF)

- IEC62443 Cybersecurity Expert

Evangelizing Security

The assignment is to act as an advocate/champion within the team to integrate security best practices into everyday workflows and development processes

Evangelizing security in the context of this mapping is a team-level assignment focused on upskilling the team, acting as a security single-point-of-contact and ambassador of the product security strategy assignment.

Together with its technical counterpart the Dev Lead, the security champion is the core security function at the team level. In many organizations, both roles/responsibilities are picked up by the same person.

Examples of roles with this assignment:

- Security Champion
- Security Engineer
- Security Ambassador

EU Cybersecurity Skills Framework: Cybersecurity Implementer

Security Skills

- Broad, High-level Security Knowledge
- Training and mentoring
- Technical Writing

Security Training Resources

- OWASP SAMM
- OWASP Security Champions Playbook
- OWASP Cheat Sheets
- Linux Foundation – LFD121 Developing Secure Software

Books

- Secure and Resilient Software Design (ISBN 9781498759618)
- Alice and Bob Learn Application Security (ISBN 9781119687405
- Real-World Cryptography (ISBN 9781617296710)
- Threat Modeling - Designing for security (ISBN 9781118809990)
- Threat Modeling: A Practical Guide for Development Teams (ISBN 9781492056553)
- Bulletproof SSL and TLS (ISBN 9781907117091)

Relevant Security Certifications

- Paul Jerimy's Certification roadmap, focus on certifications relevant to the competence area, eg. SW development, cloud, network, …
- (ISC)² – CSSLP (Certified Secure Software Lifecycle Professional)

Cybersecurity Regulatory Compliance

The assignment is to ensure that the organization adheres to relevant laws, regulations, and industry standards, thereby avoiding legal penalties and protecting its reputation.

Ownership of cybersecurity regulatory compliance is found in the legal & compliance team, often assisted by the CISO and product security functions. Personnel with this assignment can help translate relevant laws and regulations into security policies, advise on legal implications of security decisions, and follow up on regulatory changes to ensure ongoing adherence to legal requirements.

Examples of roles with this assignment:

- Legal Counsel
- Compliance Officer

EU Cybersecurity Skills Framework: Cyber Legal, Policy and Compliance Officer

Security Skills

- Knowledge of regulations
- Compliance management

Security Training Resources

- Courses from the EIPA (European Institute For Policy and Administration)

Books

- Cybersecurity Law (ISBN 9781119517323)
- Data Privacy and GDPR Handbook (9781119546095)

Relevant Security Certifications

- IAPP – CIPP (Certified Information Privacy Professional)

Product Ownership

The assignment is to define the vision and strategy for a product, prioritizing features and requirements and guiding the development team to deliver value to customers and stakeholders.

Product ownership and similar assignments might not be "security-focused" but need to be fully supportive of security efforts if these are to succeed. They need to facilitate the integration of security requirements into the product development lifecycle, prioritize security features in the product backlog and ensure that security considerations are addressed during planning and development.

Examples of roles with this assignment:

- Product Owner
- Product Manager
- Business Analyst

EU Cybersecurity Skills Framework: N/A

Security Skills

- Understanding market cybersecurity demands
- Technical understanding of product architecture, including security considerations

Security Training Resources

- High-level knowledge of security standards (ETSI / IEC / NIST..)
  eg. NIST SP800 series, IEC62443-4-2, ETSI 303645
- High-level knowledge of applicable regulations
  eg. GDPR, HIPAA, PCI/DSS, EU CRA, EU NIS2
- OWASP ASVS

Books

- Alice and Bob Learn Application Security (ISBN 9781119687405

Relevant Security Certifications

- Paul Jerimy's Certification roadmap, focus on security certifications adjacent to project and product management, applicable to the product type

Security Awareness and Training

The assignment is to educate employees about potential cyber threats and safe practices, empowering them to recognize and respond appropriately to security risks, enhancing overall organizational security.

This assignment is held by very different roles depending on the type and size of organization. It can be found within a security group, within the engineering department or HR.

Examples of roles with this assignment:

- Product Security Officer
- Security Trainer
- Human Resources

EU Cybersecurity Skills Framework: Cybersecurity Educator

Security Skills

- High-level cybersecurity knowledge
- Cybersecurity awareness, education and training programme development
- Knowledge of cybersecurity-related certifications

Security Training Resources

- N/A

Books

- The Security Culture Playbook (ISBN 9781119875239)

Relevant Security Certifications

- N/A

Technical Leadership (Dev Lead)

The assignment is to guide the development team by providing technical direction, ensuring that projects are executed efficiently and align with architectural standards and business goals

In context of this mapping, the dev lead assignment can be considered the technical part of the security champions role.

They ensure secure coding practices are followed, integrate security tools into the development pipeline and conduct code reviews. If the assignment is split out as a separate role, they need to collaborate closely with the security champions to address and remediate security issues promptly during the development process and together with the security champions, act as a liaison with the security team.

Examples of roles with this assignment:

- Technical Lead
- Lead Developer
- Principal Developer
- Security Champion

EU Cybersecurity Skills Framework: Cybersecurity Implementer

Security Skills

- Advanced proficiency in programming language(s)
- Knowledge of code quality and standards, including secure development
- Security aspects of specific development frameworks and tools

Security Training Resources

- OWASP SAMM
- OWASP Cornucopia
- OWASP DevSecOps Maturity Model
- OWASP Cheat Sheets
- OWASP ASVS
- Linux Foundation – LFD121 Developing Secure Software

Books

- Secure and Resilient Software Design (ISBN 9781498759618)
- Alice and Bob Learn Application Security (ISBN 9781119687405
- Real-World Cryptography (ISBN 9781617296710)
- Threat Modeling - Designing for security (ISBN 9781118809990)
- Threat Modeling: A Practical Guide for Development Teams (ISBN 9781492056553)

- Bulletproof SSL and TLS (ISBN 9781907117091)

Relevant Security Certifications

- Paul Jerimy's Certification roadmap, focus on certifications relevant to the competence area, eg. SW development, cloud, network, …
- (ISC)² – CSSLP (Certified Secure Software Lifecycle Professional)

Offensive Security Testing

The assignment is to identify vulnerabilities in systems and applications by simulating real-world cyberattacks, enabling the organization to proactively fix security weaknesses before they are exploited.

Penetration testing is a capability most often sourced externally at lower maturities, before building out an in-house capability as the organization's security capabilities increase.

Examples of roles with this assignment:

- Penetration Tester
- Security Tester

EU Cybersecurity Skills Framework: Penetration Tester

Security Skills

- Knowledge of penetration testing tools
- Vulnerability assessment and reporting
- Exploitation techniques

Security Training Resources

- OWASP – Web Security Testing Guide (WSTG)
- Hack The Box
- "Metasploit Unleashed" by Offensive Security

Books

- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (ISBN - 9781118026475)
- The Hacker Playbook 3: Practical Guide To Penetration Testing (ISBN - 9781980901754)

Relevant Security Certifications

- Paul Jerimy's Certification roadmap, focus on certifications in the "Security Assessment and Testing" domain
- Offensive Security – OSCP (Offensive Security Certified Professional)
- GIAC – GPEN (GIAC Penetration Tester)
- HackTheBox - HTB CPTS (Certified Penetration Testing Specialist)

Defensive Security Testing

The assignment is to proactively identify and mitigate security weaknesses by maintaining threat intelligence, vulnerability assessments and incident response capabilities.

In the context of this mapping, this assignment has overlap with both Offensive Security Testing and Security Operations, as it touches aspects of regular quality assurance, security analysis and security operations. The assignment differs from Offensive Security Testing by focusing on proactive measures and detection capabilities. It is distinct from the Security Operations assignment by focusing more on the product/application level, ensuring products and applications have the necessary capabilities to be integrated well into Security Operations.

Examples of roles with this assignment:

- Security Analyst
- Security Tester
- QA Engineer

EU Cybersecurity Skills Framework: (imperfect match) Cyber Threat Intelligence Specialist

Security Skills

- Threat intelligence
- Monitoring and incident detection
- Incident response

Security Training Resources

- OWASP SAMM
- MITRE ATT&CK – Framework for Defense
- OWASP Web Security Testing Guide
- OWASP Security Shepherd
- OWASP ASVS

Books

- Security Chaos Engineering: Sustaining Resilience in Software and Systems (9781492070931)
- Defensive Security Handbook: Best Practices for Securing Infrastructure (9781491960387)

Relevant Security Certifications

- Paul Jerimy's Certification roadmap, focus on certifications in the "Security Assessment and Testing" as well as "Security Operations" domains

- Entry level: CompTIA CySA+ (Cybersecurity Analyst)
- GIAC – GCIH (GIAC Certified Incident Handler)
- ISC2 – CISSP-ISSEP (Certified Information Systems Security Professional – Concentration in Information Systems Security Engineering)

Vendor Management

The assignment is to maintain the reliability of the supply chain by overseeing the selection, negotiation, and ongoing relationships with external suppliers, ensuring they meet the organization's demand while adhering to strict quality, cost, and security standards.

Vendor management is crucial to implement the D-SR-B stream, "Supplier Security"

Examples of roles with this assignment:

- Vendor Manager
- Procurement Manager
- Contracts Manager

EU Cybersecurity Skills Framework: N/A

Security Skills

- Knowledge of relevant cybersecurity standards
- Third party security assessments
- Knowledge of typical cybersecurity provisions in vendor contracts

Security Training Resources

- High-level knowledge of OWASP SAMM
- SANS whitepaper - Get the Risk Out! How to Manage Third-Party Cyber Risk

Books

- Third-Party Risk Management: Driving Enterprise Value (ISBN 9781118084436)
- Vendor Management: Using COBIT 5 to Manage Vendor Risk (ISBN 9781604204782)

Relevant Security Certifications

- TPRI – C3PRMP (Certified Third Party Risk Management Professional)

Build system and automation

The assignment is to harmonize build processes by standardizing tools and workflows, enabling continuous integration and continuous deployment (CI/CD) while embedding security testing and quality gates at relevant stages.

Depending on the organization, this can be a shared assignment in the team, a team level role or even a separate team. In the context of this mapping, we recommend that a dedicated person takes up the assignment, especially in organizations where the build system and pipelines are shared between multiple teams.

Examples of roles with this assignment:

- Lead Developer
- Devops Engineer
- Build & Release Manager

EU Cybersecurity Skills Framework: N/A

Security Skills

- Security in CI/CD pipelines
- Securing infrastructure
- High-level knowledge of automated security scanning and testing
- Software-Bill-Of-Materials and related concepts

Security Training Resources

- OWASP DevSecOps Maturity Model
- OWASP Cheat Sheets
- Jenkins – Pipeline as code

Books

- The Phoenix Project, A Novel about IT, DevOps, and Helping Your Business Win (ISBN 9780988262591)
- Agile Application Security: Enabling Security in a Continuous Delivery Pipeline (ISBN 9781491938843)
- Securing DevOps (ISBN 9781617294136)

Relevant Security Certifications

- Paul Jerimy's Certification roadmap, focus on certifications in the "Security Architecture and Engineering" domain
- Practical DevSecOps - CDP (Certified DevSecOps Professional)
- Microsoft - AZ-400 (Microsoft Certified: DevOps Engineer Expert)

Security Operations

The assignment is to monitor and manage the organization's security infrastructure, detecting and responding to threats in real-time to protect assets, data, and systems from cyberattacks and breaches.

This assignment is often found with the infrastructure team in smaller organizations, and moves out to a separate team in larger or more mature organizations.

Examples of roles with this assignment:

- Security Engineer
- Security Analyst

EU Cybersecurity Skills Framework: Cyber Incident Responder

Security Skills

- Incident response expertise
- Knowledge of monitoring and detection tools
- Network security expertise

Security Training Resources

- SANS Whitepaper – Guide to Security Operations
- MITRE ATT&CK – Framework for Defense
- TryHackMe - SOC Level 1

Books

- Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases (ISBN 9781717813307)
- Cybersecurity Ops with Bash (ISBN 9781492041337)

Relevant Security Certifications

- GIAC – GSOC (GIAC Security Operations Certified)
- Certified SOC Analyst (CSA) – EC-Council

Infrastructure

The assignment is to provide and maintain the foundational technology systems—including hardware, software, networks, and data centers—that enable all other business functions to operate effectively and efficiently.

Depending on the organization, this role has overlap with build automation and security operations. In the context of this mapping, we are looking for the assignment of managing the hardware, operating systems and networks that underpin development, deployment and operations of applications in scope of SAMM.

Examples of roles with this assignment:

- System Engineer
- Devops Engineer
- Operations Engineer

EU Cybersecurity Skills Framework: N/A

Security Skills

- Systems and infrastructure security (including automation)
- Network design and management
- Cloud security

Security Training Resources

- Pluralsight - Infrastructure as code: The Big Picture
- Linux Foundation - Linux Security Fundamentals
- OWASP - Top10 Proactive Controls
- OWASP - Docker Top10
- OWASP DevSecOps Maturity Model
- OWASP Cheat Sheets

Books

- The Practice of System and Network Administration (ISBN 978-0321919168)
- Site Reliability Engineering: How Google Runs Production Systems (9781491929124)
- UNIX and Linux System Administration Handbook (ISBN 9780134277554)

Relevant Security Certifications

- ISC2 – CCSP (Certified Cloud Security Professional)
- Paul Jerimy's Certification roadmap, focus on certifications in the "Security Architecture and Engineering" domain