CYRIS360

Product Security

March 2024 – Version 1.2

Unleashing Cyber Resilience in Every Direction.

In this Presentation

Overview

01 Why product security matters?

02 Generic services:

- 02.1 Threat Modeling & Secure SDLC
- 02.2 Cloud security posture management (CSPM)
- 02.3 API Security

03 Sector-specific services:

- 03.1 Automotive
- 03.2 Internet of Things (IoT)
- 03.3 Industrial automation and control systems

1. Why product security matters ?

Product security focuses on the security of the product from early stage of design and development, until the EOL. In particular, the software may run on a non-trusted environment. Think of connected vehicles, smartphones (and all associated apps), network, TV, printer, IoT, or connected devices used in manufacturing and critical infrastructure.

When compromised these may be used to attack other targets in vicinity or to execute coordinated DDoS attacks. To address these threat scenarios, the entire product design, development and implementation process shall be performed with security in mind.

2. Generic services

2.1 Threat Modeling & Secure Software Development Lifecycle

In partnership with IriusRisk

Step 1 **Design**

Security requirements
Threat Modelling

STRIDE(-LM) Methodology
Shostack's 4 Question Frame
- What are we working on?
- What can go wrong?
- What are we doing about it?
- Did we do good job ?

Step 2 **Implement**

Code Review (SAST, DAST, Secret scan)
Software Composition Analysis (SCA)

Step 3 **Build & Release**

Application Signature
Secret Management

Step 4 **Operate**

Vulnerability Management
Application/API Monitoring & Testing

2.2 Cloud Security Posture Management (CSPM)

Container Security

Vulnerability Management, K8s, Network configuration.

Chaos Engineering

Building self-healing capability into the cloud via experiments.

Identity & (Privilege) Access Management

Least privilege, Four eye principle, Authentication & Authorization.

Incident Detection & Response

Logging & Monitoring, Instance isolation, Recovery & Resilience.

CIS Center for Internet Security® Creating Confidence in the Connected World.

CSA cloud security alliance®

2.3 API Security

In partnership with CEQUENCE

API Spyder

Attack surface discovery

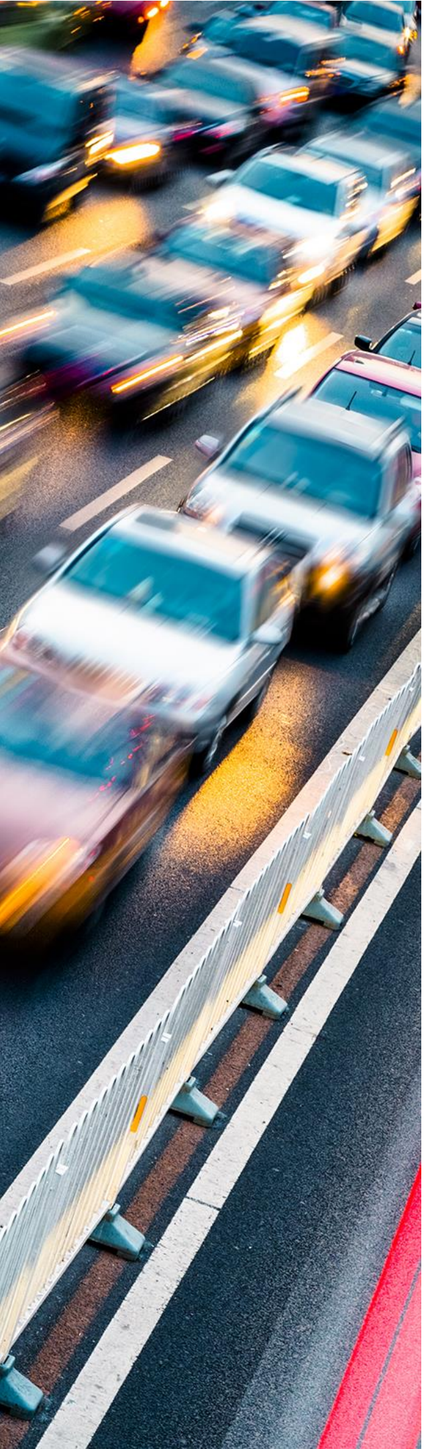
API Sentinel

Security Compliance & Testing

API Spartan

Bot Management & Fraud prevention

3. Sector-specific services



3.1 Automotive

UN regulations 155 and 156 released in 2021 and already applies to new type approval since July 2022, and will apply to all new cars from July 2024.

ISO/SAE 21434 (CSMS)

- Defines the requirements of the Automotive CSMS in 15 Clauses
- The cybersecurity case shall be maintained and may be used as a proof
- Uses a risk-based approach

ISO 24089 (SUMS)

- Defines the requirements of the Software Update Management System
- Only applicable if (part of) the software can be updated over-the-air.
- Defines the Rx Software Identification Number (RxSWIN)

In partnership with SANEON Consulting | Engineering | Solutions

3.2 Internet of Things

Standards & Regulations

- **Relevant EU Regulation**:
  Radio Equipment Directive (RED),
  Cybersecurity Act (EUCC),
  Cyber Resilience Act (CRA)
- **Relatable standards**:
  ISO/IEC27402, ETSI EN 303 645,
  EN17927 (SESIP)

Conformity assessment

- **Evaluation methods**:
  Default: (Basic) Self-assessment
  Important: 3rd party assessment
  Critical: EUCC certification
- **Target of Evaluations**
  Consumer: Doorbell, home appliance, IP Camera, Printer, Inverter, etc.
  Enterprise: Smart cities, Smart Grid, Manufacturing, Telemetry, V2X, etc.

3.3 Security for industrial automation and control systems

ISA/IEC 62443 Framework

- 14 Standards / Technical reports, organized into four parts:
  - General
  - Policies & Procedures
  - System
  - Components & Requirements
- Defines 5 Security levels (SL0 to SL4)

Conformity assessment

- **ISA/IEC 62443-4-1**: Secure product development lifecycle requirements
- **ISA/IEC 62443-4-2**: Technical security requirements for IACS components

Do you have any questions?

Let us know: we are happy to help!

info@cyris360.com

www.cyris360.com

CYRIS360