Secure by Design

Prevent issues from becoming incidents

Alex Kreilein
Vice President, Product Security

Alex Kreilein

Vice President
Product Security

Industry Experience

- Veteran CISO
- Product Manager
- Security Researcher
- Venture Investor & Advisor

Skills

- Product Security
- Cloud + DevSecOps
- Capability Maturity
- Automation
- Resiliency Engineering

Focus Areas

- Product Security
- Infrastructure as Code
- Chaos Engineering
- Continuous Validation
- Developer Productivity

Career Highlights

Qualys.

RapidDeploy
CLOUD AIDED DISPATCH™

NIST

secure|set

50+
Products Built & Secured

200+
Processes & Controls Automated

100+
Instructed

130+
People Led, Managed, & Mentored

"You do not rise to the level of your goals. You fall to the level of your systems."

– James Clear, Atomic Habits

Security Is A:

Foundational architecture pillar

Functional and
non-functional requirement

Culture and a practice

State of Secure by Design Today

Qualys.

Problems Space

Issue	Security will be in Phase 2 Security vs. Speed and Cost	We need these EoL components Service-specific architecture awareness	Security testing starts at the end Insecure default configurations
Impact	**Late-stage remediation at high risk**	**High exposure with low MTTD**	**Low security efficacy with high friction**

CISA Secure by Design Pledge

Qualys signed the voluntary CISA Secure by Design Pledge,
focused on enterprise software products, establishing that we will make good-faith effort to work towards the following goals.

Pledge Goals

01	Increase the use of Multi-factor authentication **(MFA)**
02	Reduce the use of **default passwords**
03	Reducing entire **classes of vulnerabilities**
04	Increase the installation of **security patches** by customers
05	Publish a **vulnerability disclosure policy (VDP)** that authorizes testing by members of the public
06	Demonstrate **transparency in vulnerability reporting** by including CEW and CPE fields
07	Increase in the ability for customers to gather **evidence of cybersecurity intrusions**

Secure by Design Goals

Reduce Classes of Vulnerabilities

Reduce the prevalence of one or more vulnerability classes, such as SQL injection or cross-site scripting, across all products.

Qualys adopted Content Security Policy to address XXS, reducing the escape rate of this CWE class by more than 60% in 1 Quarter.

Security Patches

Organization make it easier for customers to install patches.

Qualys became a CVE Numbering Authority (CNA) and launched its PSIRT to expedite patches.

Delivered **Shift Left** program for Qualys Engineering.

Vulnerability Disclosure Policy

Vendors should publish a vulnerability disclosure policy that gives researchers a safe way to report vulnerabilities to the vendor.

Qualys PSIRT supports responsible disclosure, vulnerability equities process, and coordination activities.

Secure by Design Goals

CVEs

Ensure accurate and timely reporting for the details of every Common Vulnerabilities and Exposures (CVE) record for their products.

Established Qualys PSIRT to escalate timely patch delivery and high-quality CVE data

Evidence of Intrusions

Enable customers to detect and understand security incidents providing customers with the logs that would assist them in gathering evidence of intrusions.

Forthcoming subscription level audit logs will be available via an API, empowering customers to detect risky behavior.

MFA and Default Passwords

Measurably increase the use of MFA across their products to get more customers to use MFA.

Within a year, reduce the amount of default passwords in their products, particularly internet-facing products.

Q1-Q2, Qualys will begin to bring foundational Identity Management Modernization improvements to GA and Public Preview.

The Qualys Secure by Design Program

Qualys

Our Secure by Design Goals

Put customer security at the center of everything we do

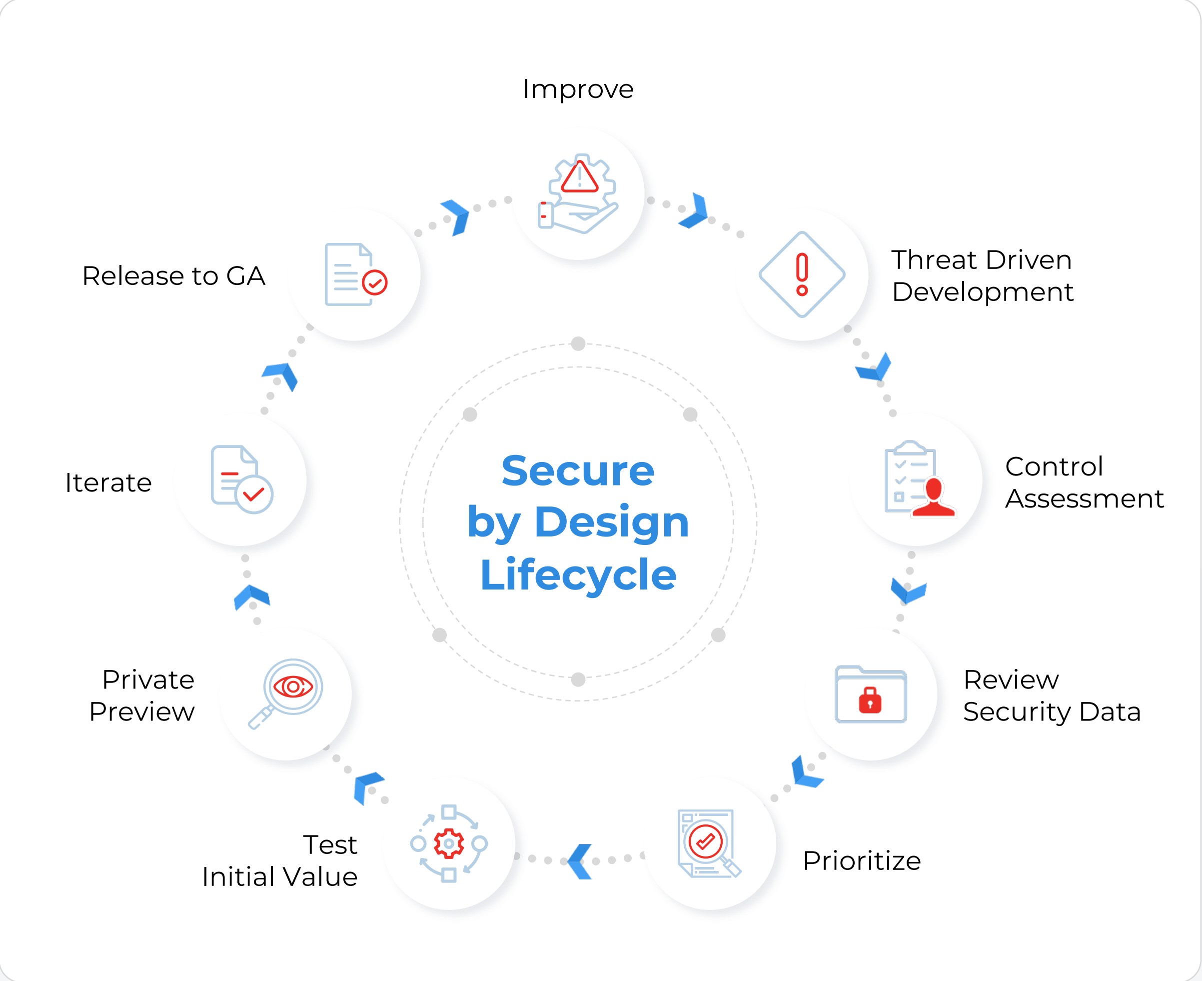
Make the secure choice the easy and default choice

Make hacking Qualys prohibitively expensive for attackers

Putting Plans To Action

The Secure by Design Roadmap Is Informed by:

- Threat Driven Development
- Security + Technical Control Analysis
- Market + Customer Feedback



Improvements Focus On:

Customer-Facing Capabilities

Internal Improvements

Secure by Design with Qualys

Identify Classes of Vulnerabilities

Web Application Security

Establish Secure by Default Configurations

Policy Compliance

Secure Configuration Assessment

Detect Production Vulnerabilities

Container Scanner

Cloud Agent

Enterprise TruRisk Management (ETM)

Secure by Design Feature Roadmap

Qualys.

Identity Security

Effective Response

Control Where It Matters Most

Security requires new systems and new operating models to deliver trust with every release

Discuss Security by Design

Qualys®