

CUSTOMER STORY

From Blind Spots to a Product Security Baseline

156 controls

scored across four pipelines

A global technology manufacturer had no dedicated product security function and needed evidence to guide investment. UltraViolet Cyber assessed four development pipelines and three flagship product families, connecting architecture risks with gaps in development practices. Leadership gained its first measurable product security baseline and a prioritized roadmap for improvement.

INDUSTRY

Technology
Manufacturing

SIZE

10,000+ Employees,
\$3.01B Revenue

ENVIRONMENT

Embedded Systems,
Firmware, C/C++

SERVICES

Application Security

— THE CHALLENGE

The manufacturer had no product security team across four development pipelines, leaving vulnerability management inconsistent. Customers wanted evidence of secure development and firmware integrity. Regulatory pressure and uneven security practices made a common baseline essential to guide investment.

— THE ENGAGEMENT

UltraViolet Cyber paired software development lifecycle maturity assessments with architecture threat modeling across four pipelines and three product families. Practitioners linked attack scenarios to mitigations and delivered an executive roadmap aligned to NIST SSDF, OWASP SAMM, and BSIMM.

— THE RESULTS & IMPACT

Leadership gained evidence to justify security staffing and governance: 156 controls evaluated, 76 attack scenarios analyzed, 37 high-priority findings (1 critical), and 17 near-term fixes identified. A roadmap and 12-month remeasurement framework support tracking progress.

MEASURABLE OUTCOMES

37 Findings

High-priority findings identified in the assessment, including 1 critical and 36 high-impact risks.

17 Next Steps

Near-term remediation opportunities identified for immediate action across the assessed environment.

76 Scenarios

Attack scenarios analyzed across hardware, firmware, and operations to guide mitigation priorities.

The assessment gave leadership a clear view of product security risk, a prioritized plan to address it, and the evidence to make the case for investing in the people and practices needed to build a repeatable program.

Continuously Assess. Consistently Defend.

Build your product security roadmap.

[View Application Security Services](#)