CUSTOMER STORY

Building the Foundation for Product Security

156 controls

scored across four pipelines

A global technology manufacturer needed to strengthen product security as customer expectations grew. UltraViolet Cyber combined development maturity assessments with architecture threat modeling to examine how products were built and where they could be compromised. The engagement gave leadership an evidence-based starting point for establishing a consistent security program across product teams.

INDUSTRY	SIZE	ENVIRONMENT	SERVICES
Technology Manufacturing	10,000+ Employees, $3.01B Revenue	Embedded Systems, Firmware, C/C++	Application Security

THE CHALLENGE

The manufacturer had no dedicated product security function, leaving vulnerability management inconsistent across development pipelines. Customers wanted evidence of secure development and firmware integrity, but leadership lacked a shared basis for evaluating readiness. The company needed to distinguish urgent product risks from organizational gaps that required clearer ownership, coordinated practices, and sustained investment.

THE ENGAGEMENT

UltraViolet Cyber assessed four development pipelines and three flagship product families, connecting architecture risks with weaknesses in development practices. Practitioners identified where teams needed specific technical mitigations and where shared process changes could address issues across products. An executive roadmap translated the findings into actionable priorities aligned to NIST SSDF, OWASP SAMM, and BSIMM frameworks and maturity models, linking immediate remediation needs with longer-term program development.

THE RESULTS & IMPACT

The assessment established a common baseline and a 12-month remeasurement framework for evaluating improvement across product teams. Leadership can use subsequent assessments to determine whether changes are addressing the identified weaknesses and where further attention is needed. This provides a consistent basis for tracking accountability, adjusting resources, and demonstrating measurable progress as the company develops its product security capabilities.

KEY ASSESSMENT FINDINGS

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.

By connecting technical findings to organizational needs, the engagement helped leadership make the case for the people and practices required to embed security into product development, with consistent expectations and clear ownership across teams.

Continuously Assess. Consistently Defend.

Build your product security roadmap.

View Application Security Services

443.351.7630 / info@uvcyber.com / UltraViolet Cyber

©2026 ULTRAVIOLET CYBER. ALL RIGHTS RESERVED.