SECURING THE DIGITAL SUPPLY CHAIN

SECURING END TO END SOFTWARE, DIGITAL AND INFORMATION SUPPLY CHAIN

AT **ORIGIN**	AT **ENTRY**	AT **IMPLEMENT**	AT **OPERATIONS**	AT **DISPOSAL**
Stage 1	Stage 2	Stage 3	Stage 4	Stage 5

ORIGIN VALIDATION	VENDOR MANAGEMENT	SECURE VALIDATION	DEMAND PLANNING	SECURE DEVELOPMENT LIFECYCLE	DIGITAL ENVELOPE VALIDATION	CONTINUOUS SECURITY OPERATIONS	ZERO DAY ACQUISITION PROGRAM	DIGITAL ASSET DECOMMISSIONING

Safeguards and Measures

• Digital BOM attestation • Independent labs • Black box testing • Code review	• Contract Management • Annual Assessment • Vendor Digital Risk Index Management • Third Party Tier 1 Vendor Assessment • Digital Bill of Material • SecOps entry exposure analysis	• Risk impact assessment • Cyber defense framework (if applicable) • Information Lifecycle Management (if applicable)	• DevOps threat modeling • Secure Coding • Security as Code measures • SAST • DAST • Penetration Testing • Digital Signature	**Multi-Layered Defense** • Secure Development Framework • Data Protection Framework • Web Application Firewall • API Security • Database Security • ETA/TLS Analysis • DDoS/Buffer/WAF • SAST • DAST • ETDR • Micro Segmentation • Layer 7 Inspection	• Parameter handling • Predictable pattern analysis • Threshold envelope learning	• Real Time Analysis • Situational Awareness • Continuous Zero Day Sensing • Threat Analysis • Insider Threat Real Time Analysis • Privilege Threat Real Time Analysis • API and Process Fork Continuous Risk Analysis • Retrospective Hunting • Continuous real time hunting • Continuous attack surface management • Exploitable chatter analysis	• Condition Assessment • Asset Disposition Risk Assessment • Business exit exposure analysis • Sanitization and degaussing processes • CMDB update • Security Operations Threat Model Update

Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software

26

CyberRes