Intel Supply Chain Overview

Matthew C Areno, PhD

Senior Principal Engineer

Nighthorse Lake and C3D Chief Architect

Office of the CTO, Intel Systems Architecture and Engineering (SAE)

Notices and Disclaimers

Intel provides these materials as-is, with no express or implied warranties.

All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No product or component can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://intel.com.

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

AGENDA

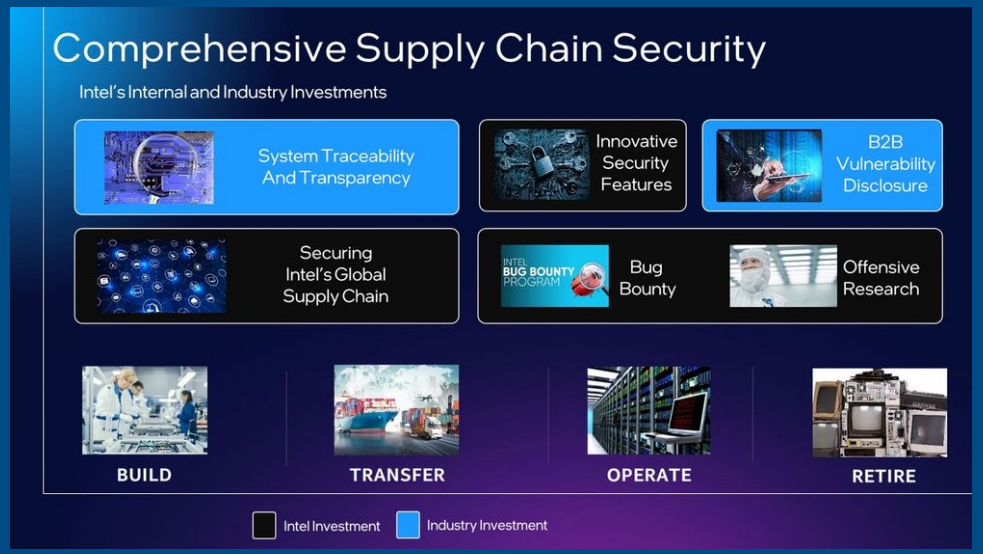
- Who's this guy
- Overview of Intel's supply chain
- Tools and Processes used
- What gaps exists

WHO AM I?

- Began career at Sandia National Labs doing nation-state level, red teaming activities.
  - Focused on reverse engineering and vulnerability exploitation work against embedded systems
- Worked for Raytheon SI-Gov/Cyber Security Innovations group.
  - SME on PRoT technologies for COTS equipment
  - Graduate of Raytheon and US Navy anti-tamper courses
- Joined Intel in 2019 and now chief architect of new high-security processing solutions
  - Former Sr Director of Security Assurance and Cryptography
  - Authored internal and external Intel documents for supply chain threat models
  - Assisting in the development of supply chain specification for ISO and USG
  - Primary interface to USG for security-related engagements

LET'S LEVEL SET

- Intel Compute Lifecycle Assurance[4] (CLA) initiative identifies four primary stages of product lifecycle:
  1. Build
  2. Transfer
  3. Operate
  4. Retire
- What standards and efforts exist today are primarily focused on Transfer and Operate phases, with little education or definition on the Build phase.
- In this presentation, we'll focus on the Build phase and how it can be assessed.



THE SUPPLY CHAIN

SUPPLY CHAIN STAGES

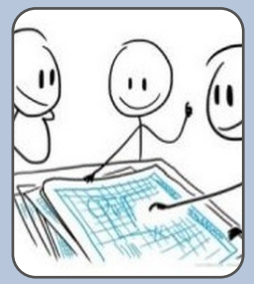
Concept

1. Define customer requirements
2. Register product into SDLe database
3. Begin product definition
4. Establish execution team and define product timeline

Development

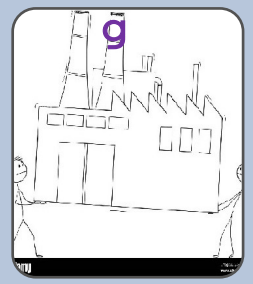
1. Create hardware and/or software design for product
2. Identify external components and providers
3. Complete internal program and security reviews

Integration



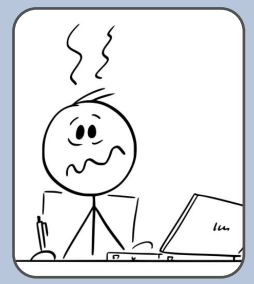
1. Integrate custom and 3rd-party components into overall design
2. Complete full system synthesis and initial testing
3. Tape-out final product and send to manufacturing

Manufacturin



1. Create product masks, typically one per layer of IC
2. Begin mass production of silicon wafers
3. Conduct wafer sort, validating structural and electrical characteristics
4. Package wafers for transfer to ATMs

Test

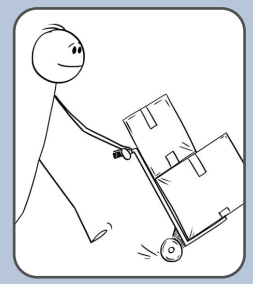


1. Products are assembled and enclosed in product packaging
2. Packaged product begins first stage testing
3. After thorough testing, product are transitioned into *high volume manufacturing* (HVM) stage

Provisioning

1. Minimal provision perform after assembly to support early product tests
2. Functional product are fully provisioned with pre-generated device data and settings
3. Final testing is performed to validate provisioning

Deployment



1. Final products are recorded in internal databases and sorted for destinations
2. Coordinate distribution of products to partners and customers
3. Manage disposal of failed products

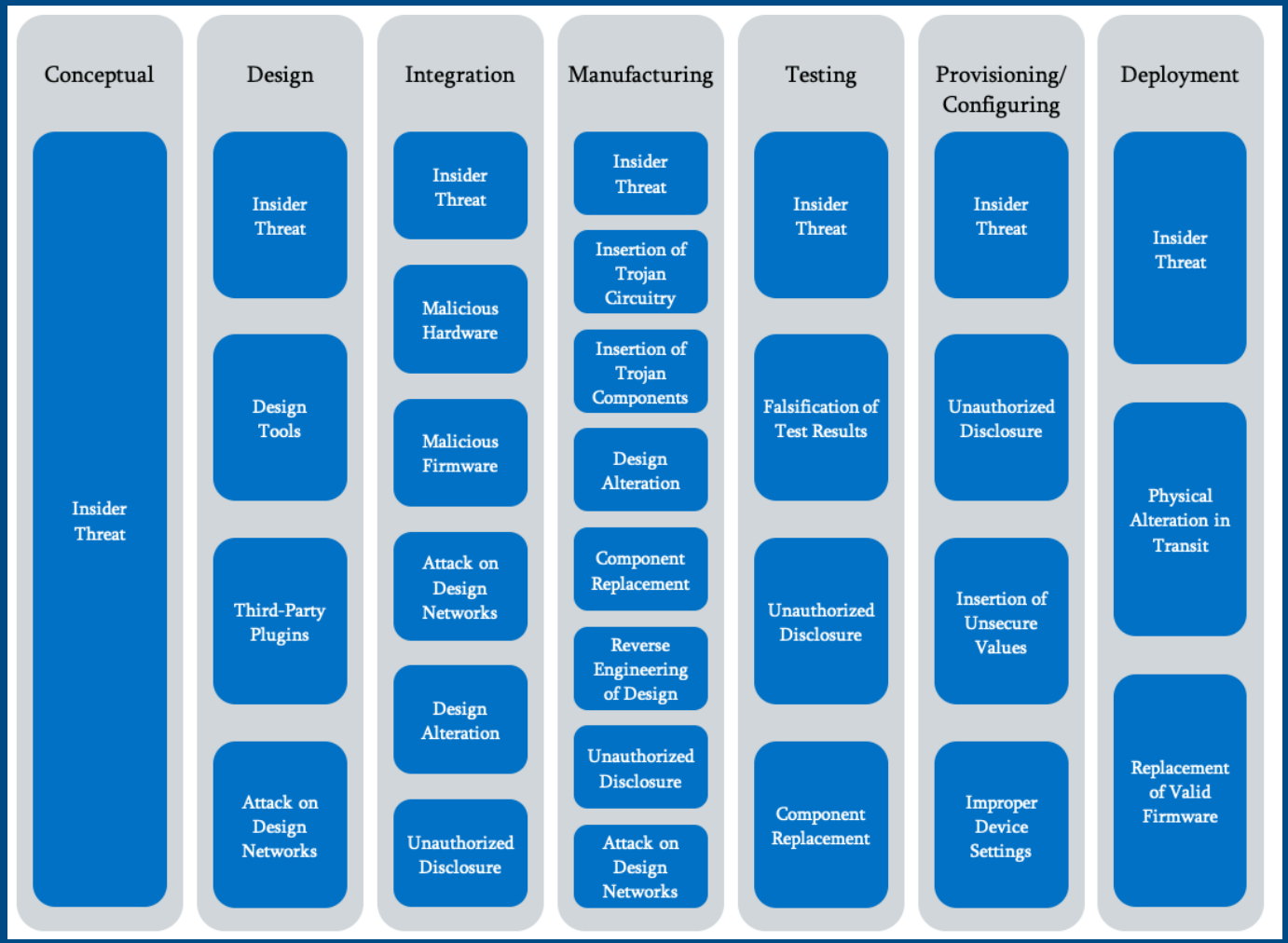
* Thanks to depositphotos.com for images

Intel Global Manufacturing Footprint

Robust, geo-diverse and expanding supply for wafer and packaging

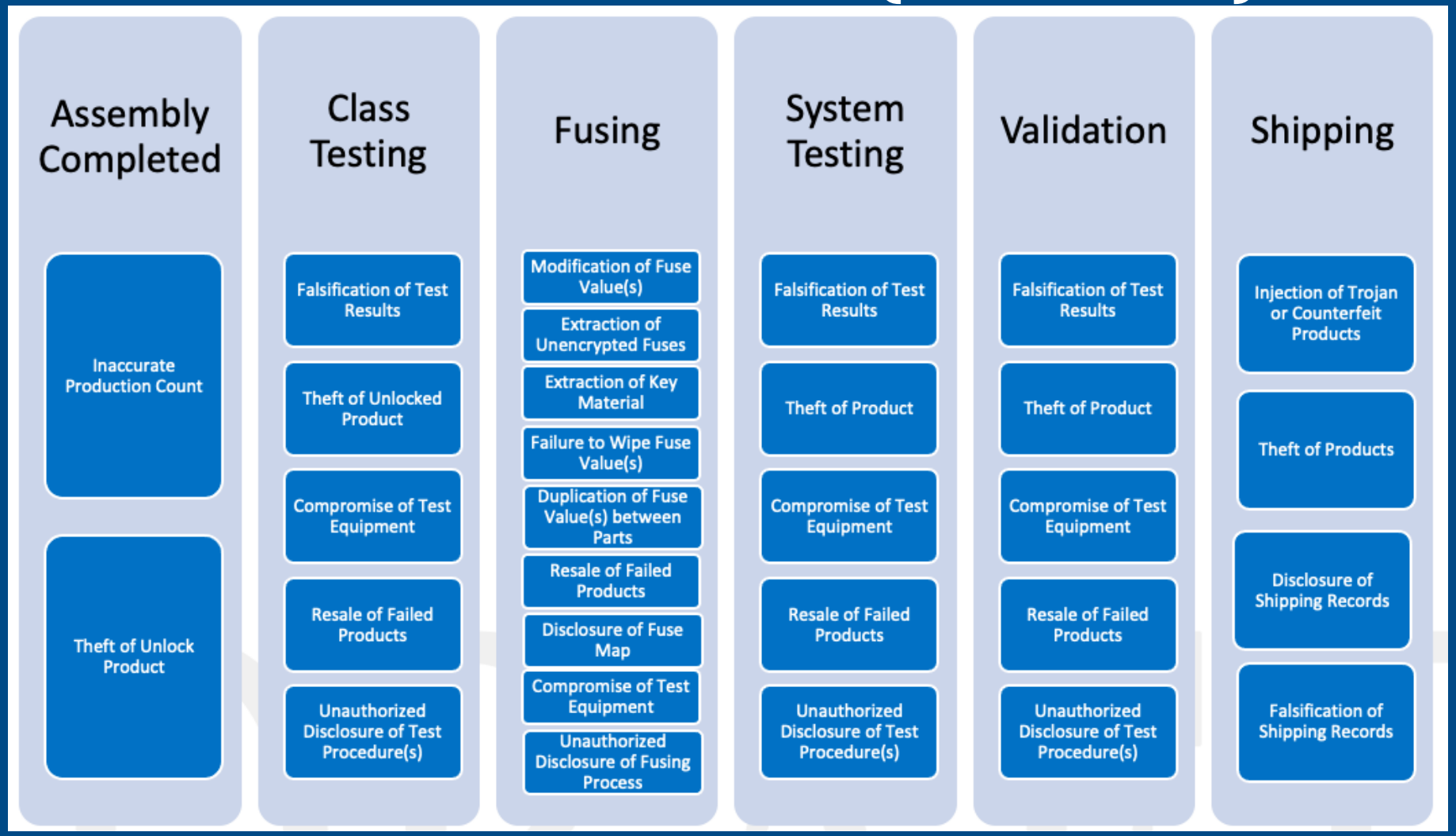
UNDERSTANDING THE THREATS

IC SUPPLY CHAIN THREATS (10K FT VIEW)

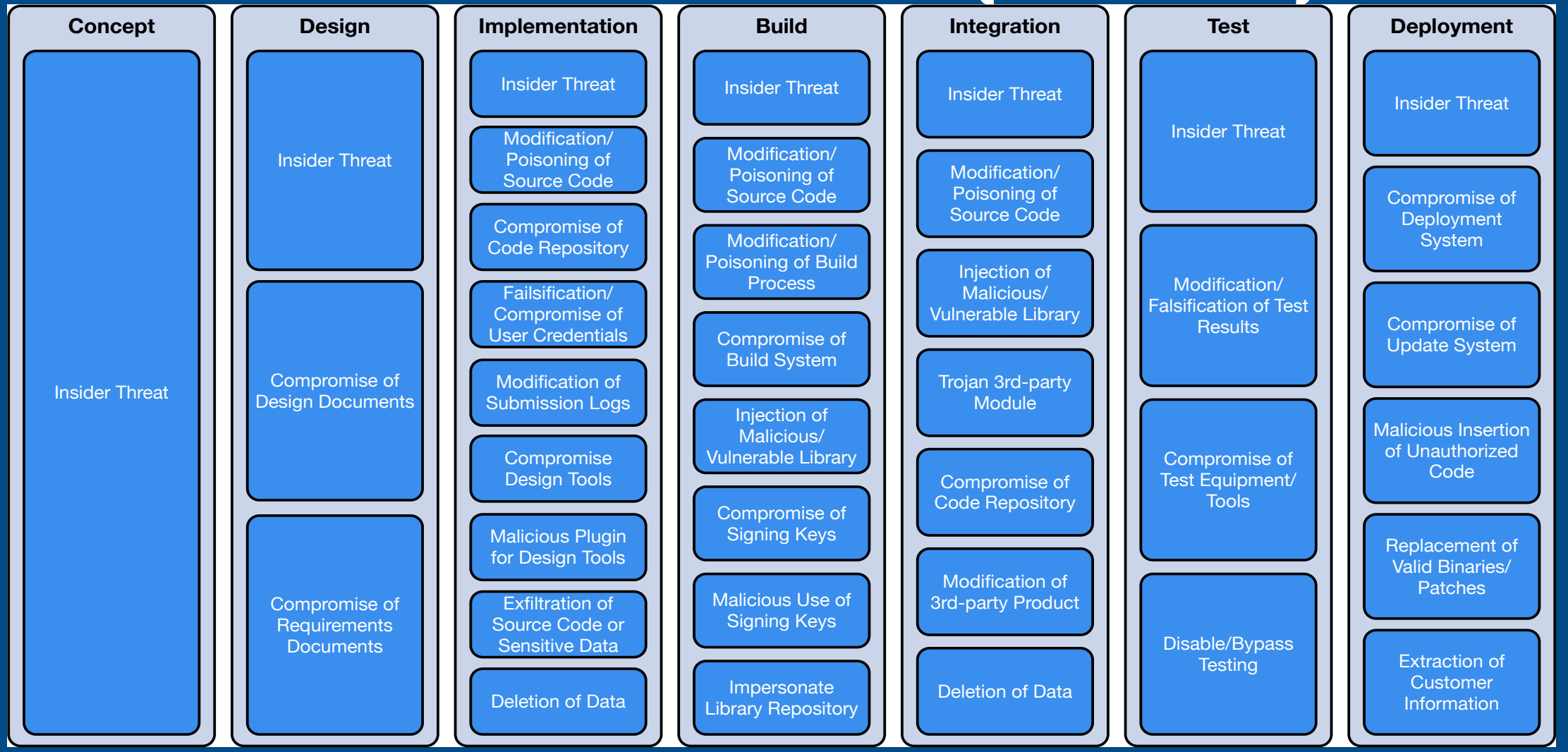


https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/supply-chain-threats-v1.pdf

KEEP DRILLING DOWN (1K FT VIEW)

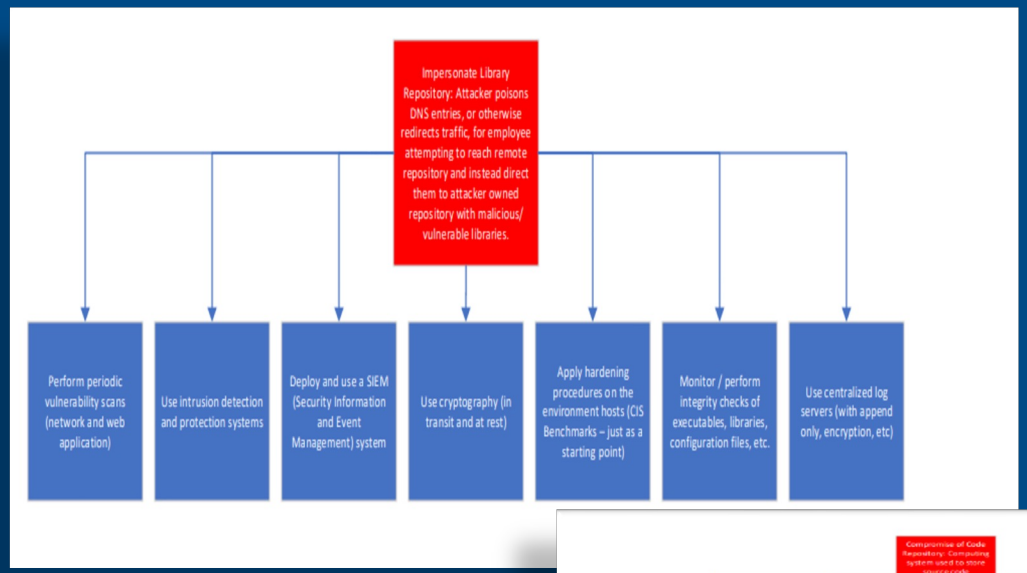


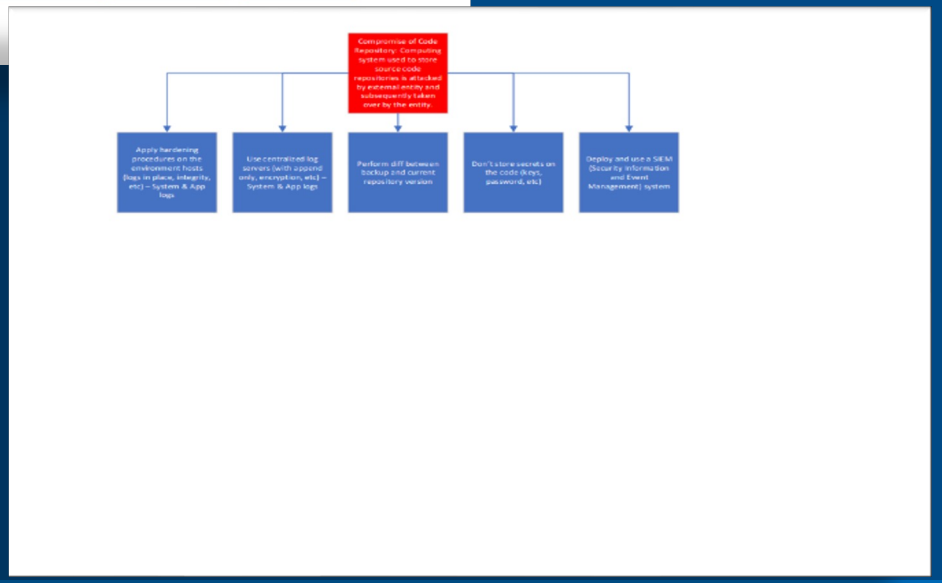
SW SUPPLY CHAIN THREATS (10K FT VIEW)



INTERNAL TOOLS

Challenge: Threats & Threat Model



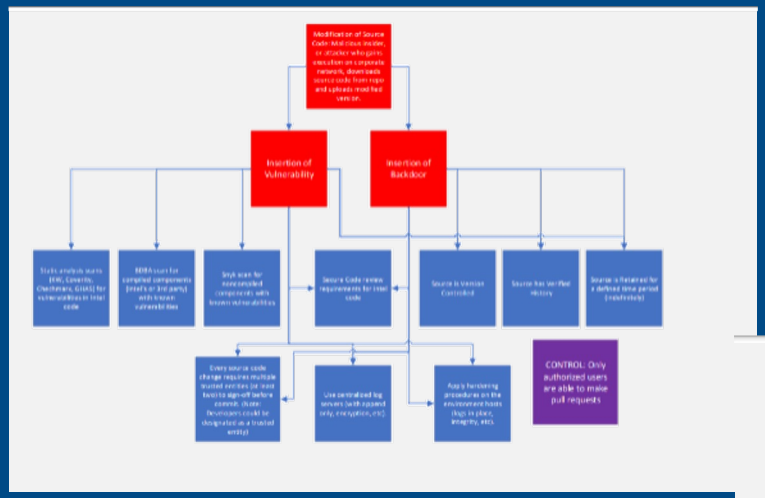


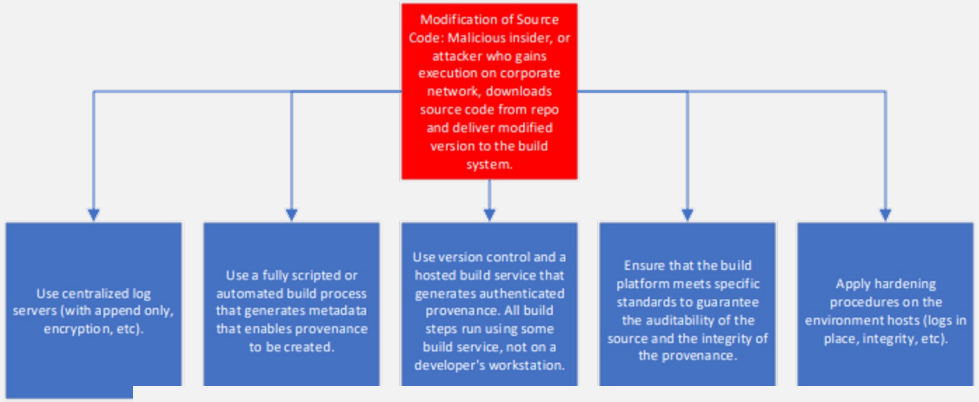
Source: Intel Supply Chain Security Experts Team

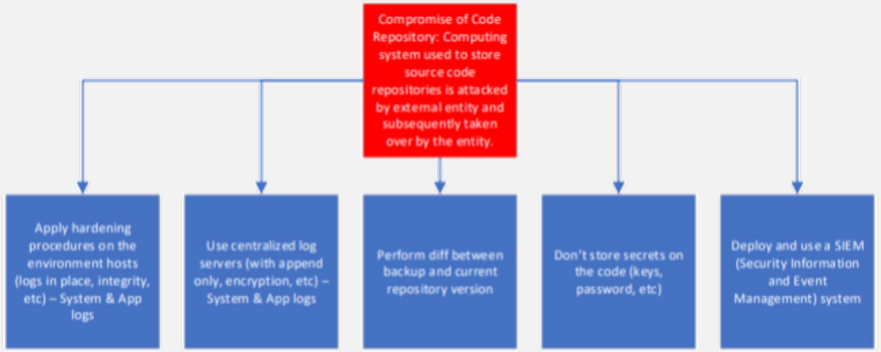
Top 25 CICD Threats

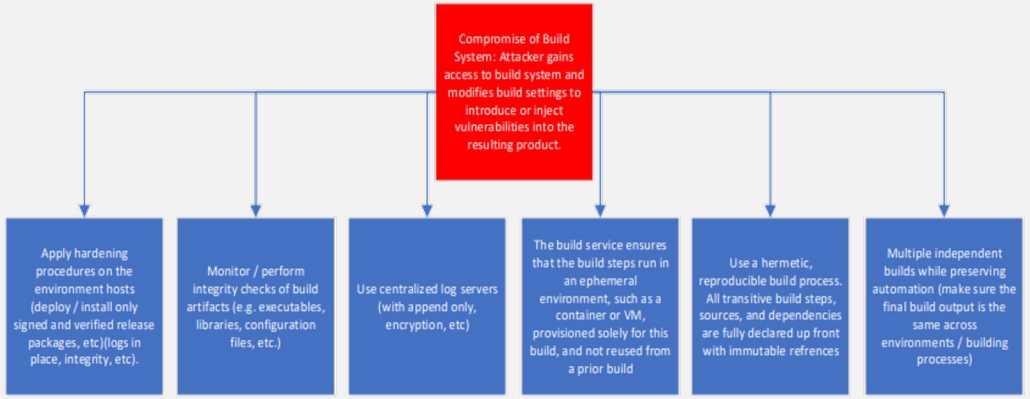
Threat ID	Threat
1	Modification of Concept/Design content
2	Modification of Requirements content
3	Exfil of Concept/Reqts/Design content
4	Modification of Source code
5	Read/Modification of Defects/Vulns
6	Compromise of Design/Dev tools
7	Exfil of Source code & Defect/Vulns
8	Modification of Source code
9	Compromise of Build system
10	Modification of binaries
11	Malicious 3PIP, Bad dependency
12	Modification/Compromise of Keys
13	Exfil of source code, 3PIP, binaries, keys
14	Modification of Test content
15	Modification/Bypass of Test results
16	Compromise of Test tools
17	Exfil of Test content & results
18	Modification of Release content
19	Read/Modification of Customer content
20	Compromise of Deploy/Update systems
21	Exfil of release content, customer content
22	Compromise of Deployed product
23	Read/modification of Defects/Vulns
24	Read/modification of Customer content
25	Exfil of Defects/vulns, customer content

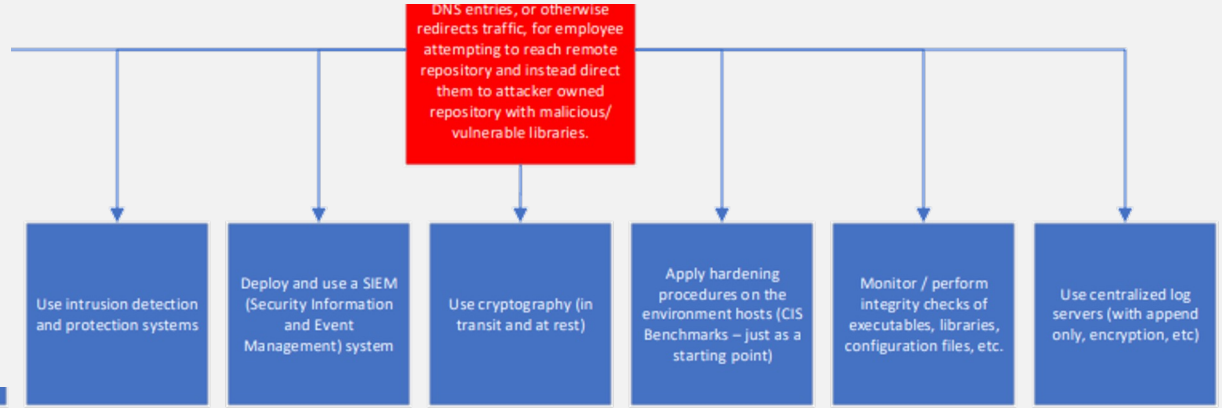
Threat Model / Attack Tree











INTEL THREAT MODELING TOOL (TMT)

- Centralized tool and threat database to assist users in the creation of robust/complete threat models
- Threat models are all stored in one location, making vulnerability triage easy and fast
- Created from the ground up at Intel

MICROELECTRONICS QUANTIFIABLE ASSURANCE (MQA)

- USG/DoD – Problem/Challenge – need to grow supplier landscape while increasing security/assurance of intellectual property (IP)
- In response to NDAA section 224, USG/DoD are defining a new framework to govern the acquisition of microelectronics products & services from commercial factories with additional assurance.
- MQA Framework foundation:
  - Applies to custom ICs.
  - Built on zero trust.
  - Designed as a supplier risk assessment model.
  - Allows for scalability – levels of assurance.
- Designed for integration with USG/DoD programs – RAMP, RAMP-C, SHIP

MQA RESULTS

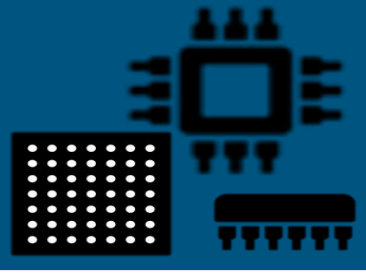
- Intel is supporting the framework development with feedback on practical implementation and pilot studies to demonstrate feasibility.
- MQA pilot demonstration helped to evaluate feasibility of MQA process in commercial foundry
- Intel comprehended MQA as part of continuous improvement foundation into its broader operations
- MQA standard can facilitate achievement of USG NDAA for quantitative assurance framework for microelectronics

INTEL® TRANSPARENT SUPPLY CHAIN HIGH LEVEL PROCESS

Data gathered and communicated on sourced components	**Creation of digital certificate for platform**	Digital certificate extended to cover full system	System authenticity verified against digital certificates

Source

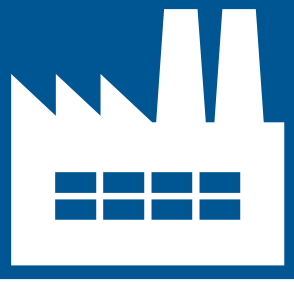
Component Data



Build

Trusted Computing Group ***Platform*** Certificate

"As Built" Data



Integrate

Trusted Computing Group ***Delta*** Certificate

"As Built" Data

Validate

Trusted Computing Group ***Delta*** Certificate

System Snapshot

Suppliers | **Manufactures** | **Integrators** | **Deployers**

PROJECT AMBER: INTEL TRUST AUTHORITY

What is Project Amber?

An Intel Service to remotely verify and assert trustworthiness of compute assets. (TEEs, devices, Roots of Trust, etc.)

Operationally independent from the Cloud/Edge infrastructure provider that is hosting confidential compute customer workloads.

- SaaS: SaaS service w/ 99.95% uptime SLA
- Multi/Hybrid cloud & Edge Support
- Intel® SGX: Multi-TEE support (Initially: Intel SGX and Intel TDX)
- Federated model for Geo-support
- VERIFIED FAITHFUL: Provable Integrity/auditability of Verification Process
- CLOUD-NATIVE: Cloud native & CSP agnostic

RELEVANT STANDARDS: NIST, DFARS, CHIPS

Entity	Description	TSC Relevance
DFARS 246.870-2	Contractors' Counterfeit Electronic Part Detection and Avoidance	• TSC aligns to DFARS
NIST SP800-161 r1	Cybersecurity Supply Chain Risk Management Practices for Systems and Organization	• TSC aligns to NIST SP • TSC highlighted in Intel/Coalfire paper
Trusted Computing Group Platform Certificate Specification v1.1	Trusted device manufacturing, traceability, and transparency	• TSC Delivers TCG Platform Certificate • V1.1 improved (April 2020) and gaining momentum
NIST NCCOE SP1800-34 (A, B, C)	Validating the Integrity of Computing Devices	• Version C (12/2022) TSC specified within "How To"
US Government CHIPs Act	Mandates plan to identify and mitigate relevant semiconductor supply chain security risks; access, availability, confidentiality, integrity, and a lack of geographic diversification in the covered entity's supply chain	• TSC aligns to SEC 103. SEMICONDUCTOR INCENTIVES Sections iii & iv page 16
NIST NCCoE Manufacturing Supply Chain Traceability with Blockchain Related Technology	Introduces the concept of a manufacturing supply chain "traceability chain," which is comprised of a series of immutable manufacturing traceability records written to industry- specific ecosystem blockchain-related technologies.	• TSC BC aligns to the manufacturing traceability with an immutable ledger technology

EXISTING GAPS/CHALLENGES

- Consistent standards for security between integrators and suppliers
- Independent verifier of vendor HW/FW authenticity
- Data model specifications for AI engines to assess supply chain security
- Tools/specifications for validating HW design compliance with security requirements

INTEL CONTACTS

- Transparent Supply Chain: Tom Dodson tom.dodson@intel.com
- Threat Modeling Tool: Jonny Valamehr jonathan.k.valamehr@intel.com
- Intel Foundry Services: Jeff Josiah jeff.josiah@intel.com
- Intel Trust Authority: Raghu Yeluri raghuram.yeluri@intel.com

Thank You!!