
2022
Product Security Report
intel security

Intel's Security-First Pledge

"The security of our products is one of our most important priorities. We strive to design, manufacture, and sell the world's most secure technology products, and we are continuously innovating and enhancing security capabilities for our products."

Pat Gelsinger
CEO

System trust is rooted in security — if hardware isn't secure, then a system cannot be secure. At Intel, our goal is to build the most secure hardware on the planet, from world-class CPUs to XPUs and related technology, enabled by software. And we have sophisticated systems to find and address security vulnerabilities in our products.

Intel's longstanding commitment to security has never been stronger. We invest in unparalleled people, processes, and products, integrating security in the ways we work and everything we work on. As we relentlessly pursue the best solutions to protect customer systems and data, you can be confident Intel is committed to:

- **Unwavering Customer Focus.** We put customer needs first in our security decisions.
- **Continuous Technology Innovation.** New threats will emerge, and vulnerabilities will be found, so Intel is committed to growing, adapting, and relentlessly advancing security.
- **Robust Incident Response.** We invest extensively in vulnerability management and offensive security research for the continuous improvement of our products.
- **Security by Design.** We follow rigorous policies and procedures spelled out in our Security Development Lifecycle (SDL) to integrate security principles and privacy tenets at every step of hardware and software development.
- **Community Advocacy.** No single entity can solve complex security challenges alone.

We actively work to deliver security without sacrificing performance. Working with our customers and industry partners, we can achieve the levels of secure performance people expect and deliver technology they trust.

To read Intel's full security-first pledge, visit: https://www.intel.com/content/www/us/en/corporate-responsibility/product-security.html

Key Findings

93%

93% of the vulnerabilities addressed in 2022 directly resulted from Intel's investment in product security assurance.

56%

137 (56%) of the 243 CVEs published in 2022 were discovered internally by Intel employees.

93%

Since the first product security report for the calendar year 2019, an average of 93% of all CVEs published were the direct result of Intel's investment in product security assurance.

85%

Of the 106 vulnerabilities reported by external researchers in 2022, 90 vulnerabilities, or 85%, were reported through Intel's Bug Bounty program.

Table of Contents

Introduction

What is product security assurance?

Product security assurance means an investment in people, processes, and tooling to develop products with security in mind, mitigate security issues before the product ships, and to expertly manage any issues found after a product is in the market.

Product security assurance means we up the ante by investing in offensive security research capabilities to hack our own products. We also conduct dozens of internal hackathon events and have an innovative Bug Bounty program to train and incentivize external researchers to hunt for bugs in our products. Through these investments, we proactively find and mitigate over 90% of the vulnerabilities we transparently disclose yearly.

Product security assurance means that our industry-leading Product Security Incident Response Team (PSIRT) manages the policies and processes to mitigate vulnerabilities efficiently. In addition, the Intel Platform Update program ensures that the entire supply chain is armed with these mitigations and ready to release them to end customers simultaneously.

Product security assurance means that the root cause of any issue found is fed back through our robust Security Development Lifecycle (SDL) to identify tooling, process, and/or training improvements needed to eliminate like issues during the product development process.

Product security assurance means Intel is equipped to provide security support to our customers throughout the products supported lifecycle. Through investments like the Long-Term Retention Lab, we physically host every Intel platform for over ten years allowing engineers remote access to these systems for security testing.

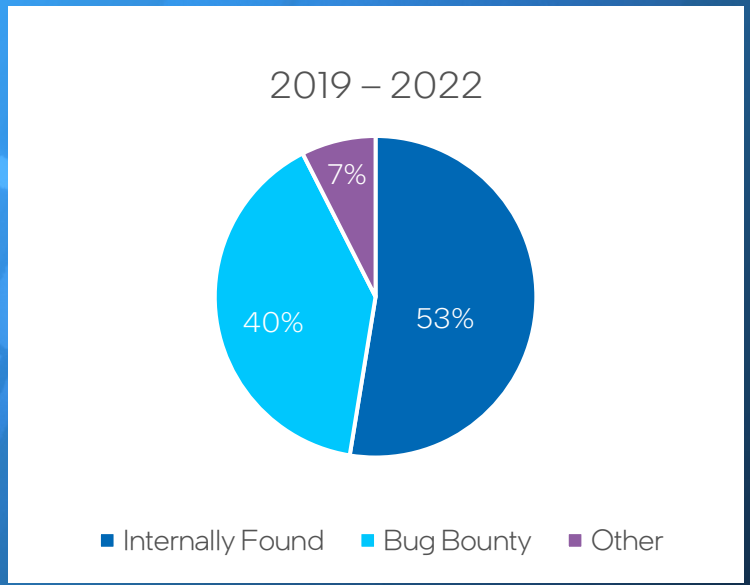
Product security assurance means that we are active outside of intel, engaging with security and academic researchers, developing new or updated security standards, leading security-focused special interest groups, and helping to inform government regulations.

Product security assurance means that customers can feel confident in Intel's Security-First Pledge and that we actively work to deliver security without sacrificing performance. By working with our customers and industry partners, we can achieve the levels of secure performance people expect and deliver technology they trust.

But most of all, at Intel, product security assurance is a mindset and an unwavering commitment to our customers.

InTechnology **Video:** Product Security Reports and CVD: Vulnerability Transparency

The Intel Product Security Report reflects our investment in product security assurance. This fourth annual report shows that Intel's proactive investments were responsible for finding and mitigating 93% of all the vulnerabilities addressed in the last four years.



Intel Approach to Cybersecurity

Suzy Greenberg
Vice President
Intel Product
Assurance
and Security

"Security is no longer a choice we make alone. If you look back at the challenges of 2018, this concept of industry and competitor collaboration has completely transformed. When it comes to cybersecurity, the technology ecosystem as a whole has really come together to collaborate through openness, trust and transparency."

Back to Table of Contents

Security-First Mindset

Security-First Mindset at Intel

Mohsen Fazlian
Corporate Vice President and General Manager, Intel Product Assurance and Security

"Implementing a security mindset often requires a shift in culture. The goal of transforming culture is to empower every engineer to incorporate security into their daily roles, be inspired to make it a personal value, and to apply security principles in what they architect, develop, validate, and manufacture."

Security-First Mindset at Intel

Four key pillars shape Intel's Security-First Mindset:

1 It starts with leadership.

Our leaders set the expectations that serve as the foundation of the culture shift, including shifting priorities around protecting data and privacy. While this starts with the executive team, others in the organization should also have insight into the potential security threats the business may face, the increasing security demands customers are concerned with, and the growing cybersecurity requirements (standards, compliance, etc.) from governments. Expectations to prioritize security throughout the business start from the top but quickly trickle down through teams. Establishing those expectations is crucial to embedding security into corporate DNA.

2 Processes and tools are the foundation.

There must be a system that can be used in non-security functions to scale the security work. At Intel, we use the Security Development Lifecycle, typically applied to software, for all product development (software and hardware). In addition, our system incorporates a network of Security and Privacy Leads, Security Champions, and Product Security Experts throughout the organization to guide our engineering and architecture teams. Finally, where possible, we incorporate tools to automate vulnerability scanning and check the security of products as they're being developed.

3 Awareness and education are essential.

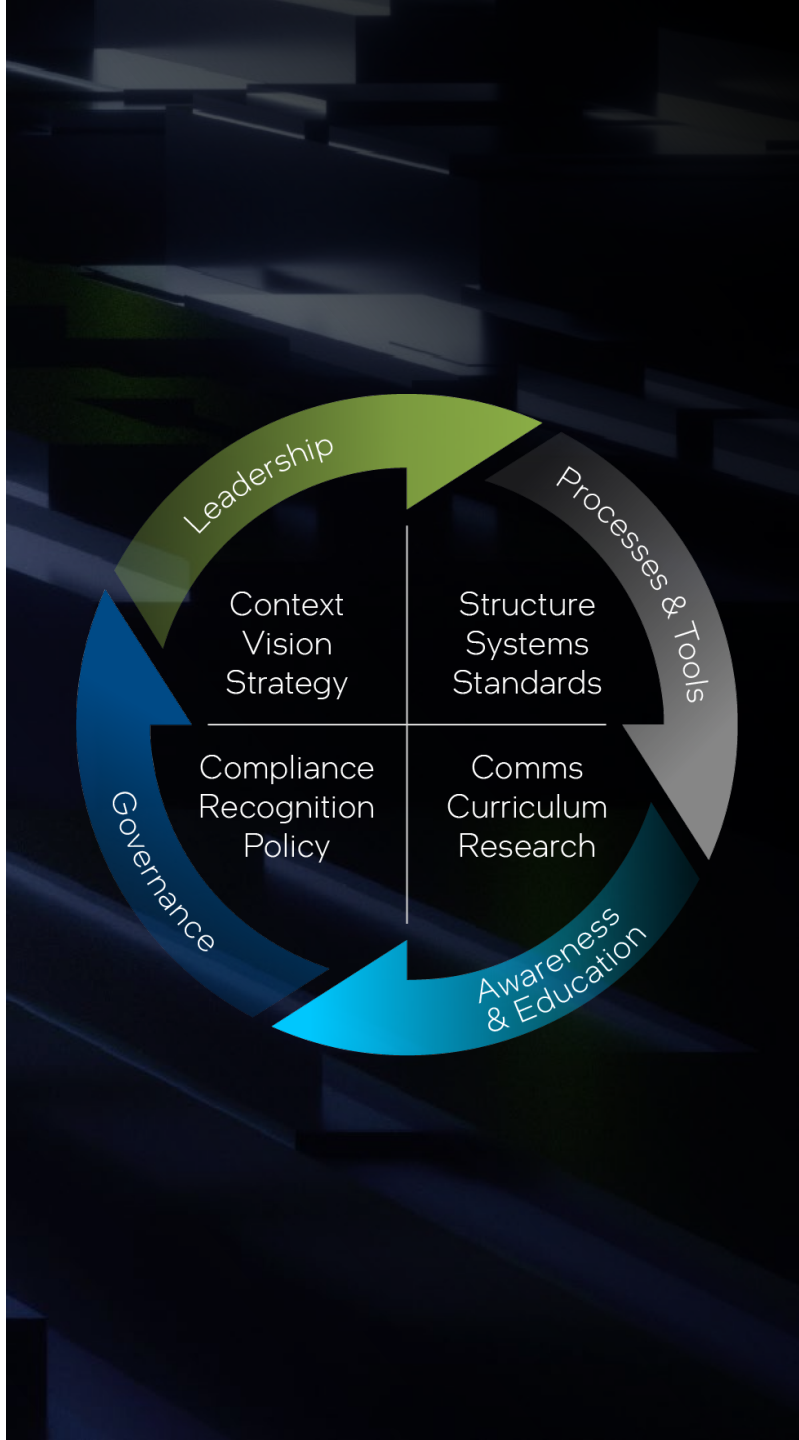
With a system in place, the next step is to inform your employees about it and train them to use the tools. The processes mentioned above introduce requirements throughout product development. Then, the network of security experts should begin working with employees to execute those requirements. They uphold this new method of development. This, along with leadership expectations and training, drives the pivot that incorporates security into how employees do their work.

Intel also incentivizes training through our Security Belt program, where employees can publicize what level of security belt they've achieved, tracking it as part of their professional development.

4 Governance, including rewards, is a necessary follow-through.

Governance may not be the first thing you gravitate to when you think of inspiring a culture shift, but it's one of the areas where collaboration can take hold. Leaders meet regularly to discuss security metrics, so all stakeholders know when issues arise.

When problems surface, Intel takes a collaborative, problem-solving approach to encourage transparency and reporting. And because people are always the most important factor, it's important to prioritize recognition as a key method of fostering the right behavior. Unfortunately, while this certainly isn't novel, those in the product security and cybersecurity worlds can get caught up in incident response and correcting issues rather than taking the time to reward the right things.



Vision

Empower our customers with the most secure systems, software, and services, driven by innovation, to enhance security capabilities they trust.

Purpose

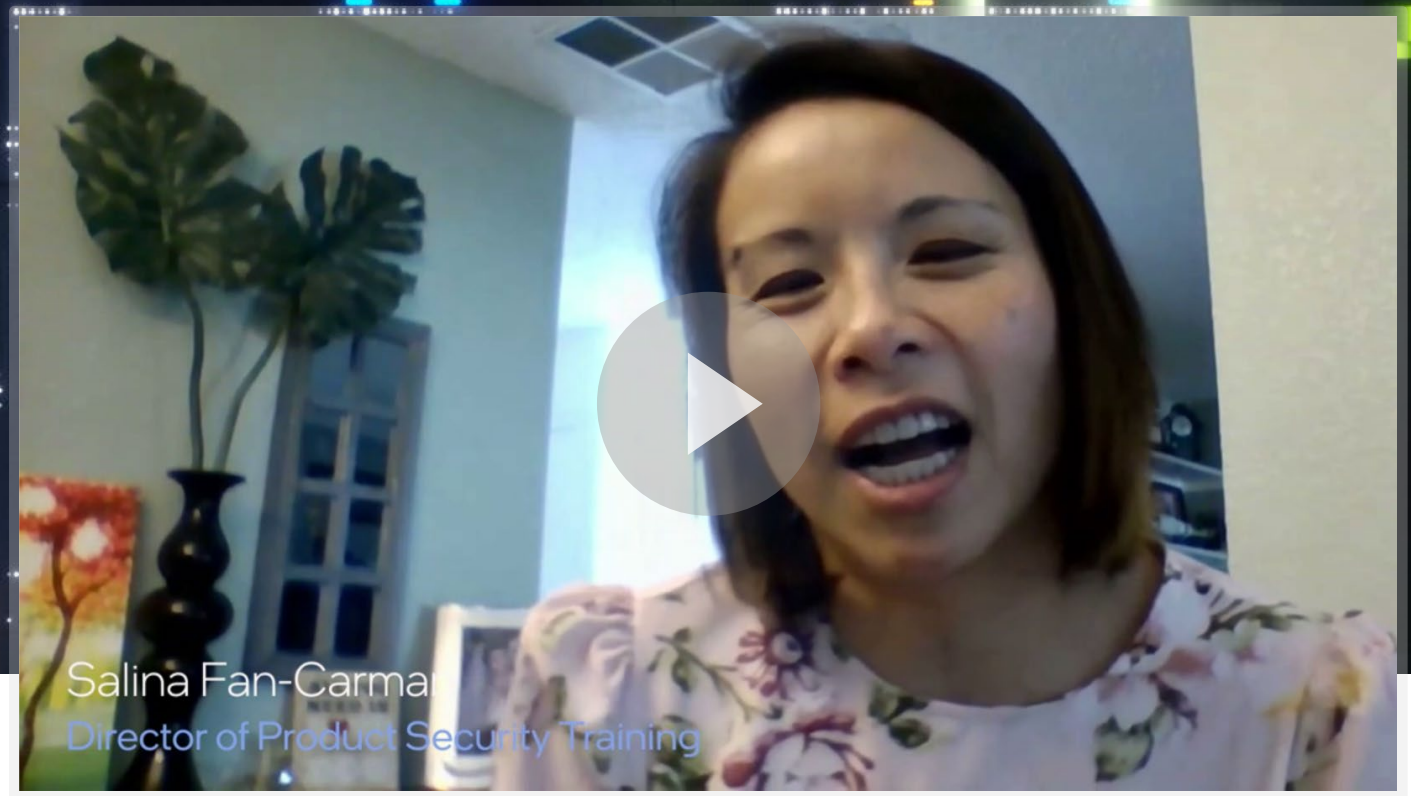
To build world-changing technology that earns trust and enriches the lives of every person on earth.

Culture

Every Intel engineer is *empowered* to incorporate security in their daily roles, *inspired* to make security a personal value, and *trained* to "think like a hacker," breaking what they make.

Security-First Mindset

Security Belt Program



Salina Fan-Carman, Intel Director of Product Security Training

As part of Intel's Security-First Pledge, we seek to increase security awareness and build skills for all Intel employees. The Intel Security Belt Certification program, launched in October 2020, is one way we strive to develop that security-first mindset measurably. Each security belt earned increases security knowledge and impacts the security of our products as well as impact across the ecosystem as our employees engage in helping to drive industry-wide initiatives and standards.

Intel Security Belt Certification

The Security Belt Certification program is a product security awareness program. The program aims to provide the knowledge and awareness for each individual at Intel to have a security-first mindset/culture to learn, act, apply, and influence to build more secure products.

Awareness

Develop an understanding of the importance of a secure development mindset and why it is critical to build security into all stages of product development.

Learner

Individuals can select hardware versus software security training pathway. They will be exposed to a fundamental understanding of SW security or HW security.

Practitioner

More advanced understanding of concept and knowledge of security, security principles, tools, techniques, and implementation in a focused area. Act upon the knowledge through Hack-a-Thon (HaT), projects, tournaments, etc.

Expert

Recognized expert in at least one technical security area. Leading Hack-a-Thons, Pen Testing, etc. Proliferate learning and knowledge to the rest of the organization.

Leader

Recognized as an established leader across the company. Broad expertise in multiple technical security areas and knowledge at a system/platform level. Identify mitigation to security findings and provide effective countermeasures.

Visionary

Recognized as security leader internally to Intel and externally in industry Broad expertise in the entire security ecosystem. Influence on principles, techniques, tools, and methodologies impact at the industry level.

MENTORS FOR LOWER BELTS

Back to Table of Contents

Product Security Assurance During Product Development

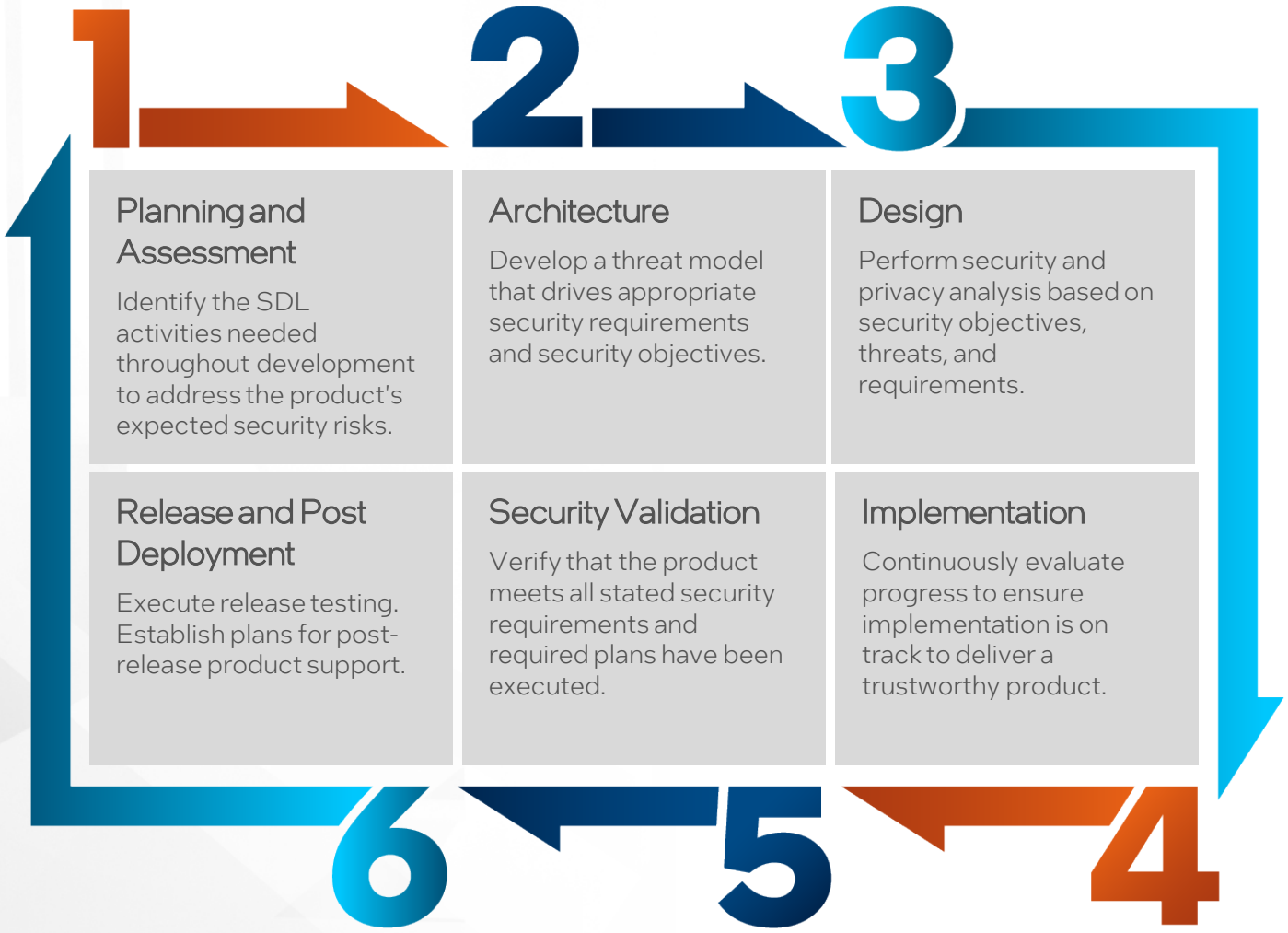
- Security Development Lifecycle
- Intel Security Hack-a-Thon (HaT)
- Security Research Team
- Intel Transparent Supply Chain
- Third Party Security Assessments

Security Development Lifecycle

Security Across Six Phases

The Intel Security Development Lifecycle (SDL) guides us in applying privacy and security practices across hardware and software (including firmware) throughout the product lifecycle. Learn more.

Diana Carroll
SDL Content Architect Intel

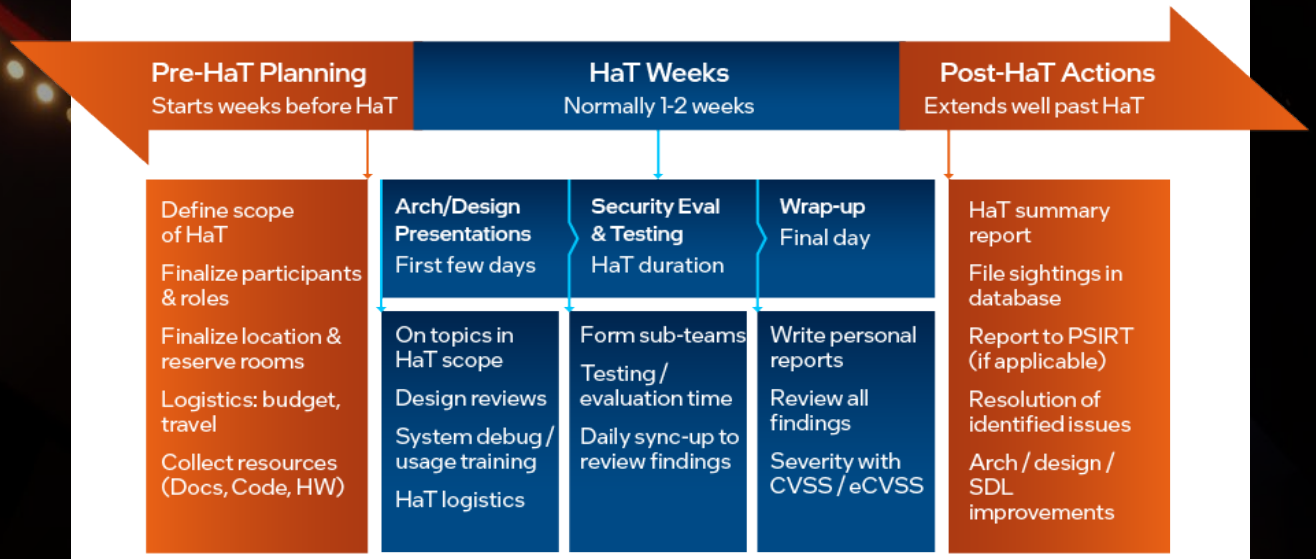


InTechnology **Podcast:** Secure Lifecycle Development (SDL)

Intel Security Hack-a-Thons (HaT)

Having a security-first mindset means that employees learn to think like hackers. To accomplish this, employees receive ongoing training and hands-on experience through scheduled HaT events. HaT events are a crucial way to bring product experts together with security experts to build a security-first mindset.

In 2022, security teams across Intel conducted 118 HaT events.



HaT Goals and Motivations

- Improve Product Security: Through security findings and mitigation and Architecture / Design hardening recommendations.
- Increase Security Know-Hows and Build Community of Practice: Through immersive, hands-on security experience for product development and security assurance teams.
- Assess Quality of Product Assurance Execution: Type of security issues, quality and quantity of issues, provide a good assessment of product's SDL execution and security capability.
- Improve Security Tools and Training: Key learning (technical and process) and application of tools are driven back to product teams as well as IPAS Governance, Tools, and Security Development Academy.
- Enable Cross-Pollination: Technologies and Security knowledge are transferred among Product and Security experts, and ongoing collaboration is established for continuous learning.

Truc Nguyen
Director, Offensive Security Research

Hareesh Khattri
Senior Security Researcher

Przemyslaw Duda
Offensive Security Researcher

Security Research Teams

iSTARE: Intel Security Threat Analysis and Reverse Engineering
STORM: Strategic Threats Offensive Research and Mitigations
OSR: Offensive Security Research

Our mission is to provide high quality research in a consumable and timely fashion to enable our customers to make the best choices for security.

80 Researchers

10 Countries

Areas of Expertise

Attacks on privileged FW
Fault injection
Formal Methods
Fuzzing
Memory Research
Microcode and Micro-architecture
Networking Technologies
Physical Attacks
Security of AI and AI to break security
Side Channels (HW & SW)
Supply Chain Security
Telemetry-based Attacks

Special Skills

Hacker Mindset
One Intel Holistic view
Industry Research
Novel SW & HW mitigation
Automation pathfinding
Embedded Cryptography

Experience

Finance
Chemistry
Validation
Design
Programming
Crypto
Academia
Engineering

Offensive Security Research (OSR)

Ensuring we are continually finding, mitigating, and reporting security issues in our products.

Proactive Research

Dedicated researchers continually monitor and probe Intel products and platforms for known, emerging, and novel threats and attacks.

- Intelligence Insights
- Architecture Reviews
- Threat Model ++
- Vulnerability and Exploitation
- Systemic Mitigations

Reactive Research

Intel acts swiftly when a new vulnerability or exploit is discovered, quickly working to develop systemic mitigations.

- Triage incoming PSIRTs
- PSIRT mitigation effectiveness

Capabilities and Culture

Solutions to instill the security-first mindset within every Intel architect, developer, designer and validator.

- Immersive Mentoring
- Security Belts
- Tools | Purple Teams
- Training | SDL

Researcher and Community Outreach

Investments to engage the global research community in industry and academia.

- Listening Events
- Research Sponsorship
- Diversity & Inclusion

InTechnology **Podcast:** Offensive Security Research; aka Hacking with Jason Fung

Isaura S. Gaeta
Vice President
Security Research,
Intel Product
Assurance
and Security

"Our commitment is to enhance the security of the entire ecosystem, benefitting our customers as well as competitors. We believe that sharing Intel's successes and learnings around security and product assurance helps our entire industry."

Intel STORM Team: Overview

Intel STORM Team: SPEAR

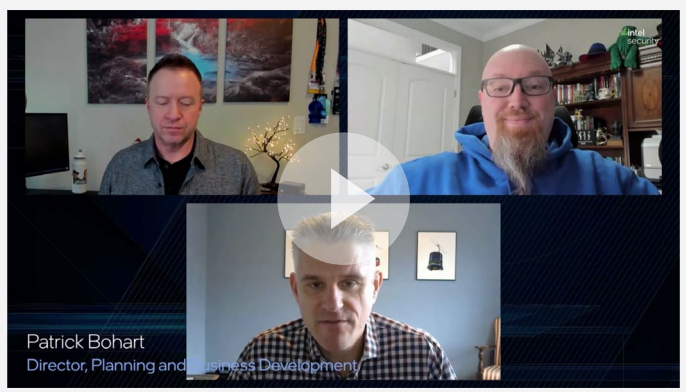
Intel STORM Team: Thais Moreira

InTechnology **Podcast:** Diversity and inclusion in cyber security

Intel Transparent Supply Chain

Intel is leading the industry in hardware supply chain assurance with Transparent Supply Chain. It's a set of tools, policies, and procedures implemented on the factory floor at PC and server manufacturers that help enable enterprises to verify the authenticity and firmware version of systems and their components.

There is growing concern that counterfeit electronic parts can cause safety hazards or failure of business-critical applications or that vulnerabilities can be introduced into the supply chain to be exploited later. Current supply chain practices start with trusting the source, but processes are limited for screening out counterfeit components, particularly for products containing many subsystems.



Patrick Bohart
Intel Director of Planning and Business Development

InTechnology **Video:** In cyber security, "due to supply chain issues" means something else

Lenovo's **LaTrea Shine** talks about Lenovo supply chain and their implementation of Intel's Transparent Supply Chain to support their customers.

Key Features

Security
Digitally signed statement of conformance for every platform attests to the platform's authenticity.

Accountability
Component-level traceability via Direct Platform Data File contains all L9 integrated components, including processor, storage, memory, and add-in cards.

Traceability
Platform certificates linked to the discrete Trusted Platform Module (TPM) provide system-level traceability.

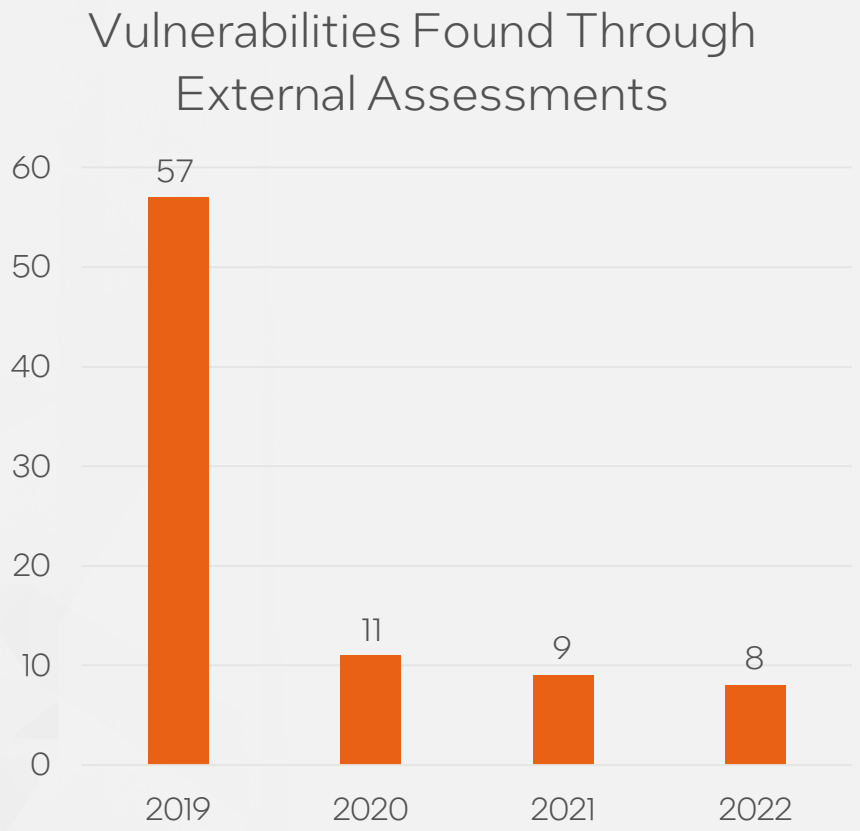
Assurance
Auto Verify tool compares the "snapshot" of the direct platform data taken during manufacturing with a "snapshot" of the platform components taken at first boot to help detect tampering.

Third-Party Security Assessments of Intel Technologies

Intel has a robust program for working with external security vendors to perform security assessments on our products. Intel's program is unique in how it's leveraged and helps ensure high-quality security assurance of Intel products.

Intel takes learnings from these assessments to increase security, quality, and influence supporting security infrastructure, like training, SDL practices, automation, and tools. Vetted and trusted security vendors contracted to provide third-party assessments not only help improve the speed of delivery of components in the Intel portfolio but also help provide vital, cutting-edge security awareness and education to our internal subject matter experts around product security.

Intel conducts yearly security assessments with external security vendors on products under development. The chart below shows the average number of vulnerabilities discovered in each assessment by year.



Back to Table of Contents

Ongoing Product Security Assurance

- PSIRT
- Intel Platform Update
- Intel Bug Bounty Program
- Technical Guidance
- Long-Term Retention Lab

Customer Spotlight: Dell Technologies

Lisa Bradley, PhD
Sr. Director, Product & Application Security
Dell Technologies

InTechnology **Podcast:** "PSIRT" with Lisa Bradley

PSIRT

Intel PSIRT Mission: Minimizing Impact Through Vulnerability Mitigation and Disclosure

The Intel Product Security Incident Response Team (PSIRT) works to minimize customer impact through mitigating and public disclosure of security vulnerabilities. Intel PSIRT supports and governs policies, processes, and guidelines for addressing security vulnerabilities that may affect Intel shipped and supported products.

Intel PSIRT

Intel's PSIRT helped define and role model industry-approved methods for how we support product engineering in the identification, management, and disclosure of security vulnerabilities that may affect shipped and supported products. PSIRT is the central point for managing Intel's response to product security vulnerabilities, including:

- Setting policy, process, and tooling to ensure consistent handling, disposition, and disclosure of product security vulnerabilities.
- Advising Intel businesses and engineering groups on product security vulnerability handling.
- Maintaining relationships with partner, customer, government agency PSIRTs, and vulnerability handling organizations.
- Creating and actively participating in industry groups and standards to help influence the creation of best practices and standards.

Intel's PSIRT holds deep industry expertise, with team members averaging 18 years of experience.

Intel Bug Bounty Program

Intel's PSIRT manages the Intel Bug Bounty program. This program provides recognition to encourage external researchers to report security vulnerabilities on Intel products and collaborate on disclosure. Intel has worked with more than 250 external researchers through the Bug Bounty program since its inception.

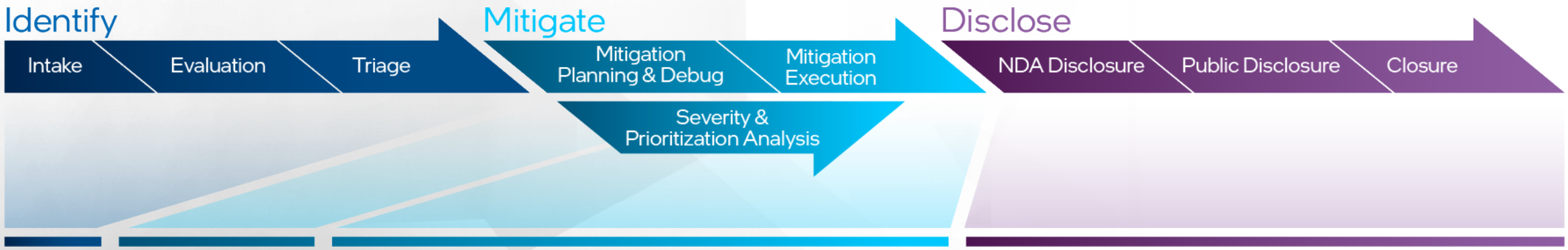
Intel's Bug Bounty includes both a continuous, public VDP program and the Project Circuit Break program. The latter is a series of targeted events such as "Show and Tell" videos, live hacking, Capture the Flag, and immersive training to build proactive, positive engagement with the security research community.

Intel PSIRT Process

Intel PSIRT outlines comprehensive and repeatable processes for addressing issues within the company. For example, potential security vulnerabilities are prioritized based on severity and impact, with handling done in three phases: Identify, Mitigate, and Disclose. Learn more.

Coordinated Vulnerability Disclosure

Intel is committed to rapidly addressing security vulnerabilities affecting our customers and providing clear guidance on the solution, impact, severity, and mitigation. Intel PSIRT policies, processes, and guidelines are designed to support and encourage the principles and practices of Coordinated Vulnerability Disclosure.



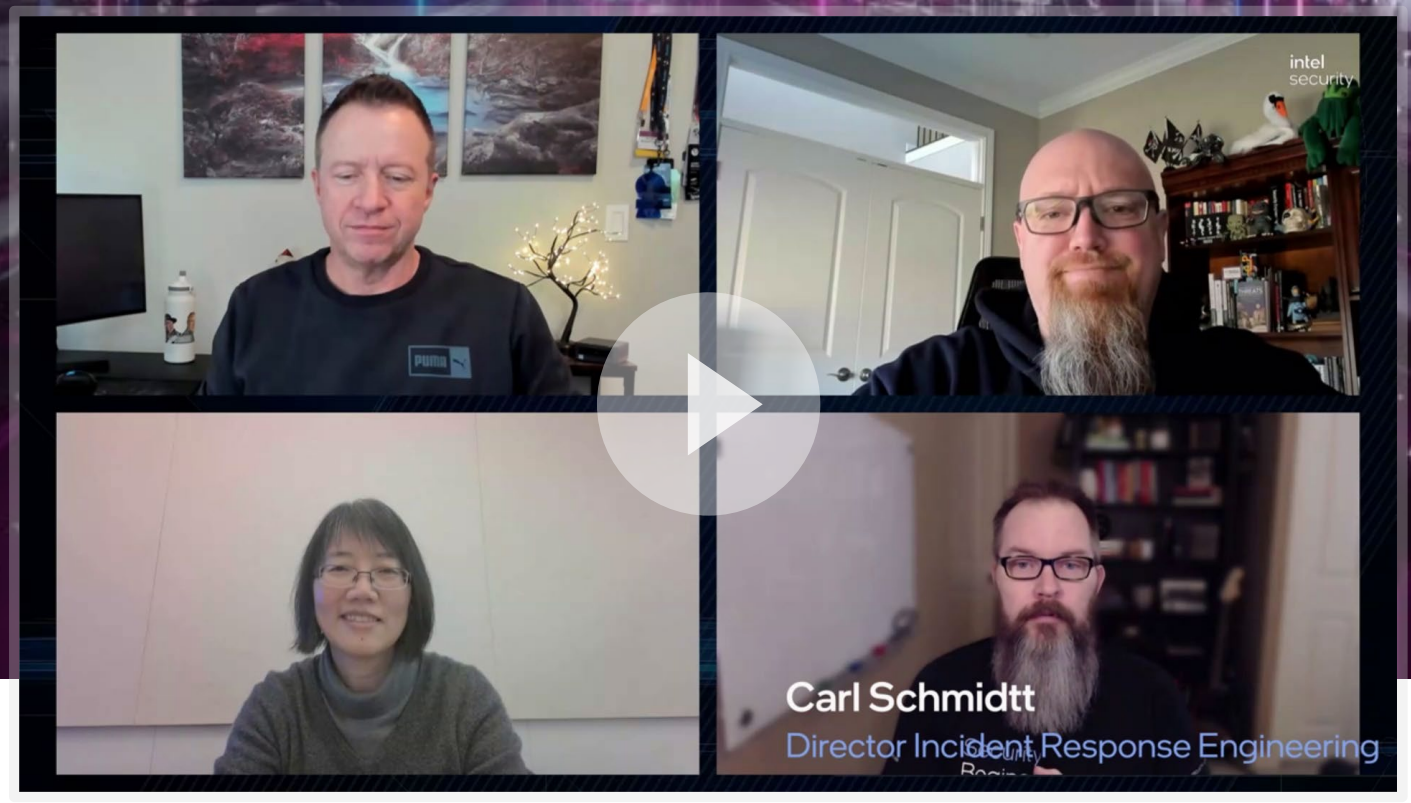
Intel PSIRT: Industry Participation

Intel PSIRT is a member of First.org and participates across many industry special interest groups (SIG) and work groups (WG).

Intel's **Josh Dembling** on the role of PSIRT

Industry				
	FIRST.Org PSIRT SIG ICASI	NIST ISO Contribution Multi-Party CVD	CVE Program PSIRT Coaches	HW CWE OSSF WiCyS

Intel Platform Update



Intel's **Zimo Ma** and **Carl Schmidt** discuss the Intel Platform Update

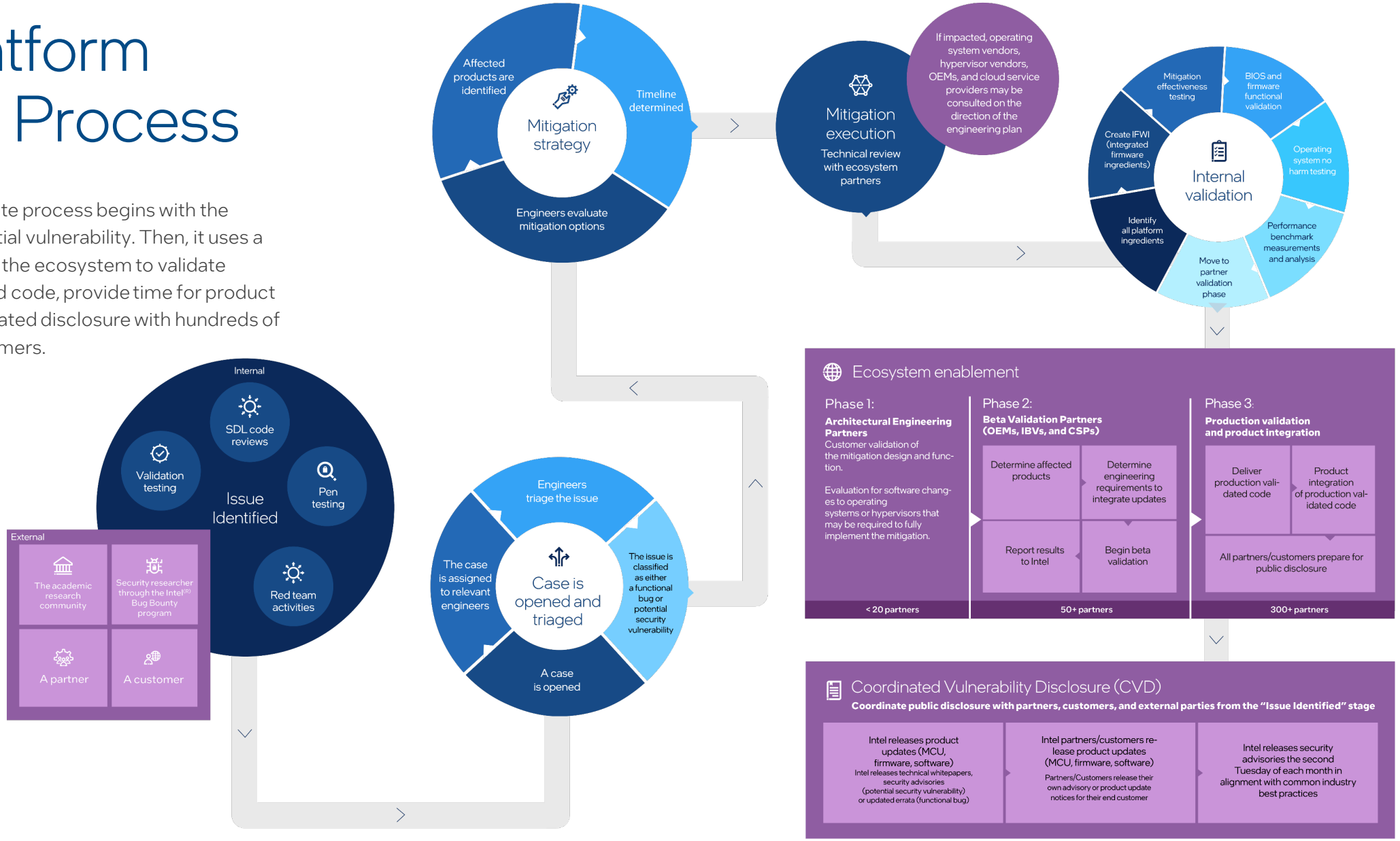
Driving a Predictable Cadence of Product Updates

As part of our drive to deliver robust product and security assurance, we regularly release functional and security updates for supported products and services.
Due to the highly integrated nature of hardware, firmware, and software, product updates often require additional validation and integration from Intel's ecosystem of partners participating in the coordinated vulnerability handling process.

Ecosystem partners include operating systems vendors, cloud service providers, independent firmware vendors, original equipment manufacturers, and systems integrators who release validated updates through direct channels to their customers. The Intel Platform Update process facilitates the ecosystem coordination and vulnerability handling process, leading to the release of validated updates.

Intel Platform Update Process

The Intel Platform Update process begins with the identification of a potential vulnerability. Then, it uses a phased approach within the ecosystem to validate mitigation strategies and code, provide time for product integration, and coordinated disclosure with hundreds of Intel downstream customers.



Bug Bounty Program

The community of security researchers from around the world continues to contribute to improving the security of technology. Collaboration on security research yields improved identification and mitigation of potential vulnerabilities, and coordinated vulnerability disclosure allows all parties time to develop and deploy mitigations. We value these contributions and aim to reward researchers through our Bug Bounty program.

More information about Intel's Bug Bounty rewards:
Intel® Bug Bounty Program
Project Circuit Breaker

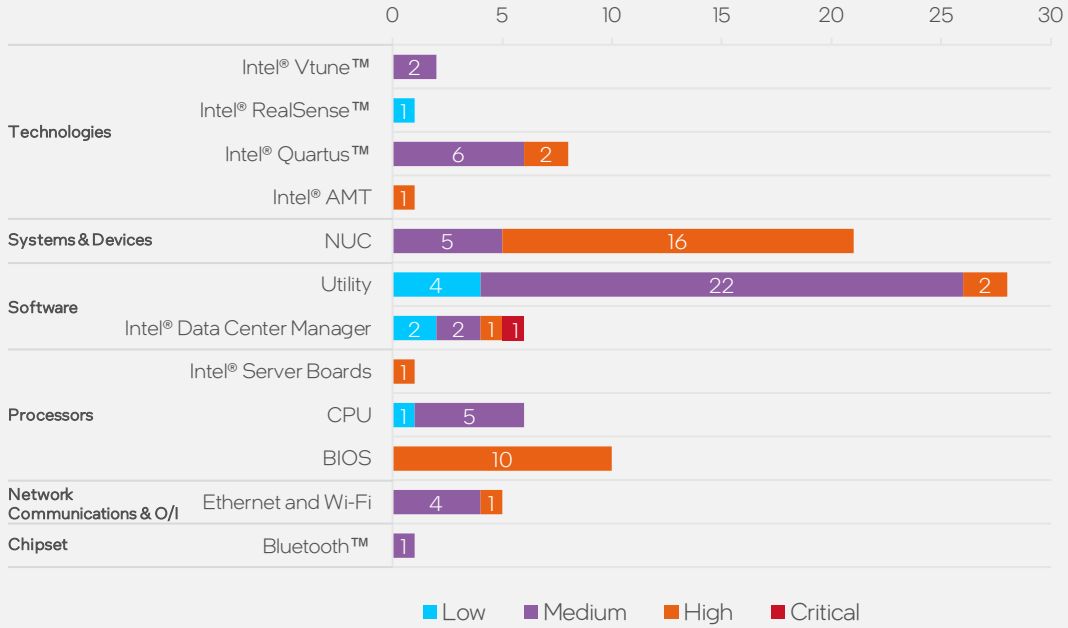
2022 Top Ten Researchers by Payout

edward
nbit
max_wang
HackingThings
Zwink
Falconcorruption
mmg
malcolmst
sheikhrishad
mohammed

Bug Bounty Submissions by Product Category and Severity

While software continues to be the primary category for Bug Bounty submissions, as we have implemented new bounty programs such as Project Circuit Breaker, we are beginning to see more external research at the firmware level, which is one of the goals of the program.

Find more information in the CVE Data section of this report.

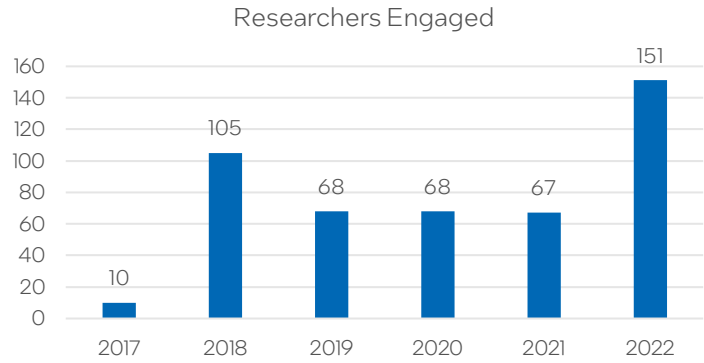


Bug Bounty Total Payout by Year

Since our public Bug Bounty program started in 2017, Intel has paid out $4,115,251 in bounties.

Unique Researchers Engaged by Year

Programs like Project Circuit Breaker (launched in 2022) are designed to engage researchers at an engineering level and draw more researchers down to the hardware layer.



Project Circuit Breaker

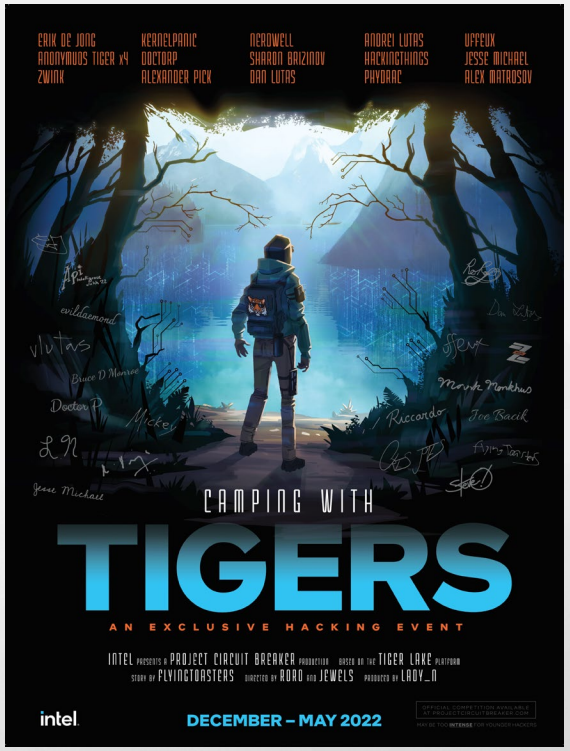
For the first time, security researchers can work directly with Intel's product and security teams through live hacking events that may include bounty multipliers. Capture the flag contests and other training will help prepare researchers for challenges, which may include access to beta software and/or hardware and other unique opportunities.

Meet the researchers where they are!

Project Circuit Breaker is

- The campaigns and events arm of the Intel® Bug Bounty program
- Focused on researcher recruiting and improvement
- Community development and support
- A newly formatted creative bounty program
- A way to drive external visibility of security research
- A unique way to recognize excellent efforts

Project Circuit Breaker 2022 Events



Camping with Tigers

This exclusive event invited select security researchers to hunt vulnerabilities in the 11th Gen Intel® Core™ vPro® platform. The six-month event included two months of training and three cycles of finding vulnerabilities, each receiving a multiplier to Intel Bug Bounty's standard bounty amounts.

Guard-en Party

We offer exclusive training events for researchers looking to deepen their knowledge of Intel products and expand their skills for hunting bugs. In the inaugural event, researchers learned from renowned academic security researchers, Intel engineers, and product security researchers. In addition, the team focused on Intel® Software Guard Extensions (Intel® SGX), an advanced, trusted execution environment technology for reducing the attack surface in the cloud.

Leveraging original proof of concept applications, participants were invited to explore exploitations using tools, techniques, and skills presented during the training sessions, like the capture the flag style challenge.

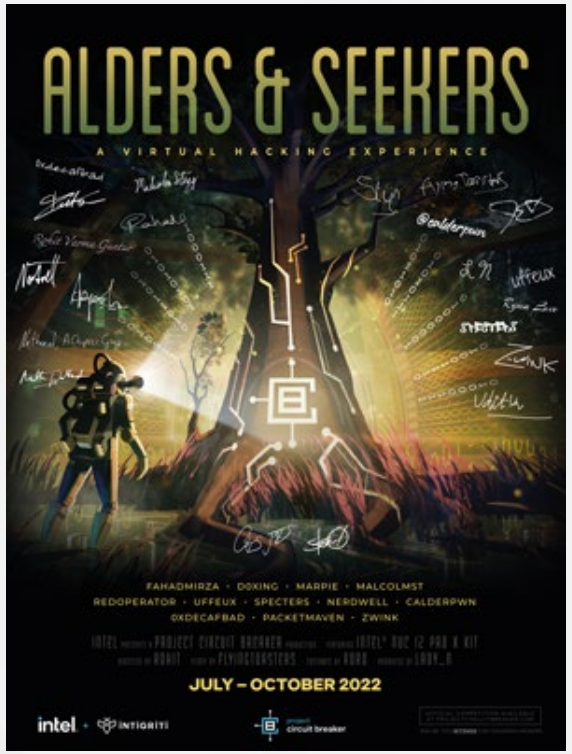
More info at www.projectcircuitbreaker.com

Project Circuit Breaker 2022 Events

Trusted Crossings

To expand security coverage, the Data Platforms Engineering and Architecture (DPEA) team, Security Assurance and Research (DSAR), partnered with the TDX team and Intel Product Assurance and Security Circuit Breakers program. Together they conducted security research twice on Intel® TDX with external security researchers named Trusted Crossings.

The new confidential computing technology will launch on Intel Xeon System on a Chip codenamed Sapphire Rapids. It is a critical security technology from Intel for cloud customers. TDX protects the confidentiality of customer workload from Cloud Service Provider. Intel recruited researchers based on their related research and an application process before granting them access to a private cloud hosted inside Intel data centers before it hit the marketplace.



Alders & Seekers

Project Circuit Breaker recruited applicants online and at DefCon30 to join us in security research against 12th Gen Intel® Core™ processors—a generation like no other before it. This was a virtual hacking experience that ran for 11 weeks where participants were invited to half a dozen training sessions alongside receiving a state of the art Intel® NUC Kit (formerly known as Dragon Canyon) including a 12th Gen Intel® Core™ desktop processor with the Intel vPro® Platform. Participants had the opportunity to test the platform, to hack it, earn bounties, meet other researchers, and get exclusive access to ask questions to Intel product and platform engineers. Alders & Seekers was later extended to include BIOS reference code that was leaked.

More info at www.projectcircuitbreaker.com

Intel Bug Bounty

Intel's **Katie Noble** and **Chris Holt** on Intel Bug Bounty programs

Security Researcher, **Sepehrdad**, on participating in the Project Circuit Breaker Trusted Crossings event

InTechnology **Podcast:** Bug Bounty/Crowd Sourced Security with Katie Noble

Technical Guidance from Intel

Microarchitectural security is a priority for Intel.

Intel is committed to supporting the software development ecosystem through the following:

- **Transparency**: We do our best to inform customers of microarchitectural issues affecting our products.
- **Software guidance:** We help software partners make informed decisions and update software as needed to mitigate relevant issues – balancing concerns about software complexity and performance considerations.
- **Hardware:** Where feasible, mitigations are supported by hardware, and speculation features can be limited or disabled.
- **Research and education:** We invest in fostering academic research and educating customers about microarchitectural security.

Intel's commitment to transparency involves documenting the architectural and microarchitectural origins of security issues, and then developing, describing, and deploying mitigations in software and/or hardware for affected processors. This transparency allows researchers, industry experts, developers, and customers to understand the root cause, whether and how the issue affects their computing environment, and what actions they need to take to address it. Researchers may use this information to focus their work better and build upon Intel's mitigations. Customers also use our documentation to understand the potential tradeoffs and implications of mitigations on their environments and workloads.

In 2022, Intel published 16 technical papers related to side-channel issues.

Paper Category	Title
Technical guidance for Intel Security Advisories	Stale Data Read from Legacy xAPIC
	Post-barrier Stack Buffer Predictions
	Return Stack Buffer Underflow
	Processor MMIO Stale Data Vulnerabilities
	Undefined MMIO Hang
	Speculative Load Disordering
	Branch History Injection
Software Security Guidance	CPUID Enumeration and Architecture MSRs
	Frequency Throttling Side Channel Guidance
	Refined Speculative Execution Terminology
	Securing Workloads Against Side Channel Methods
Hardware Features and Controls	Data Operand Independent Timing Guidance
	Fast Store Forwarding Predictor
	Data Dependent Prefetcher
Mitigation Research	You Cannot Always Win the Race: Analyzing the LFENCE/JMP mitigation for Branch Target
	Intel Research on Disclosure Gadgets at Indirect Branch Targets in the Linux Kernel

Annie Leong
Security Program Manager

Long-Term Retention Lab

Intel realized a need to preserve platforms and their respective design collateral and create a system for teams to track and identify what's being kept in various locations. By storing products and information about configurations, Intel scaled its engineers' ability to analyze security and functional issues on supported products more efficiently while better enabling proactive research for the continuous improvement of products.

When the lab started, the main goal was to create a centralized location for storing hardware; this later expanded to retaining thousands of live platforms along with design, software, and documentation collateral. These systems are available to Intel engineers around the globe 24x7 and can be made ready for testing in a matter of minutes.

Key Stats

Over

5,500

boards covering 100 platform families

35K

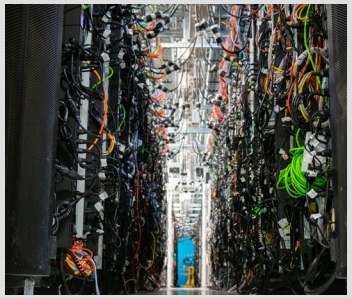
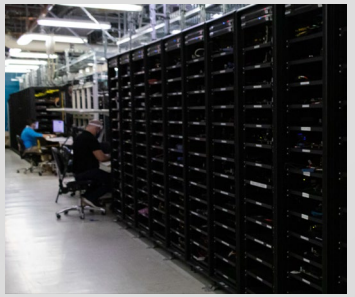
silicon items in inventory for product support

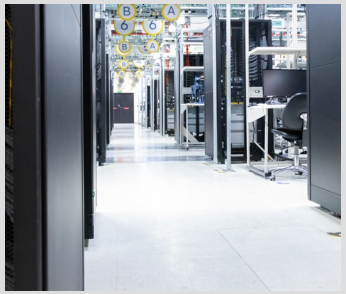
Oldest product:

Bloomfield

Newest platforms:

Catlow



Intel's **Vivek Tiwari** and **Fawn Taylor** about the implementation and operation of the Long-Term Retention lab.

Back to Table of Contents

How Intel Engages the Ecosystem

- Academic Research
- Open Source Software
- Community and Policy Advocacy
- Industry Engagement

Academic Research

Collaboration with the research community through academic investment and partnerships is critical for fueling new ways of thinking to address current and future security threats. Our relationships with leading security research institutions allow us to work with top talent across various programs.

The following are some of Intel's academic research programs. Learn more.

Sponsored Research

Intel invests directly in proactive security research, collaborating with leading institutions and academic researchers in areas of mutual interest. These areas include:

- Resilient Architectures and Robust Electronics
- Private AI Collaborative Research Institute
- Crypto Frontiers Research Center
- Scalable Assurance
- Intel Collaborative Research Institutes – Safe Automated Vehicles
- Side Channel Academic Program

Research Experience for Undergraduates

Intel coordinates Research Experience for Undergraduates (REU) Programs, partnering with leading academic institutions to provide hands-on guidance to help students gain experience in security and privacy research. REUs also build a more diverse and inclusive talent pipeline.

Awards and Recognition

The Intel Academic Excellence awards seek to highlight researchers making an impact on the security and trustworthiness of the computing ecosystem, tackling complex problems, and who are increasing the participation of women and underrepresented minorities in computer science and engineering. The four categories are:

- Hardware Security Academic Award
- Outstanding Researcher Awards
- Academic Leadership Awards
- Rising Stars Faculty Awards

Researcher in Residence

The Researcher in Residence program allows university professors to take a sabbatical from their university work so that they can work side-by-side with Intel's security researchers, taking advantage of Intel's lab facilities and capabilities. In 2022, the first program candidate, Professor Yossi Oren, was co-located with the Intel iSTARE team.

Intel's **Jason Fung** on Intel's academic programs and awards.

Researcher in Residence
Professor Yossi Oren

2022 Intel Hardware Security Test of Time Award Winners

2022 Intel Hardware Security Academic Award Winners

2022 Research Experience for Undergraduates
Priya Naphade

InTechnology **Video:** Intel Academic Leadership award winners in 2021 talk about hardware Capture the Flag

InTechnology **Video:** REU: hear directly from former student participants

Open Source Security

Open Source Software (OSS) has grown in prominence over the years and has become a key source of innovation and ideas for the industry. Intel has been a contributor to OSS for over 20 years, both within our product portfolio and in critical upstream ecosystems.

Intel participates at all levels of the software stack, including:

- Integrated OS and application frameworks
- Cloud, edge, and data center projects
- Browsers and Web-Runtimes
- Machine Learning and AI
- Networking, storage, and databases
- Graphics and media
- Virtualization
- Kernel/OS
- Firmware
- Tools and SDKs

Key Stats

Intel has invested in hundreds of open source projects over the last

20 YEARS

In the last 5 years, Intel has invested

$250 MILLION in open source security

Intel is the

#1 CORPORATE CONTRIBUTOR

to the Linux Kernel

Community Leadership

Intel has been a founding member and major contributor to many of the core security-focused groups working to improve the whole open source ecosystem. Our work within these foundations allows us to have a broad positive impact for all stakeholders. While each group has a different focus and projects, they all aim to uplift the security of open source software for all producers and consumers.

Our work at the Open Source Security Foundation (OpenSSF) spans multiple efforts, and all focused on improving the security of how open source software is created, maintained, and delivered throughout software supply chains.

Our work in the Confidential Computing Consortium (CCC) is key to furthering security in cloud and computing that requires high degrees of assurance and security.

The Cloud Native Computing Foundation (CNCF) is focused on cloud, containers, and hyper-scaling workloads across multiple cloud-based networks.

Open Source Leadership with **Arun Gupta**

Overview of Intel's Open Source security efforts with **Antonio Gomez**

Bill Roberts on TPM2 for Linux and other Open Source security projects

Tamas Lengyel is the lead developer for KF/x, the maintainer of Xen, LibVMI, DRAKVUF, and the chief research officer at the Honeynet Project

Pawan Gupta, Linux Kernel engineer working on hardware vulnerabilities, Linux security modules, virtualization, and device drivers.

"I fundamentally believe in an open source bias, which powers the software-defined infrastructure that transformed the modern data center and ushered in the data-centric era."

Pat Gelsinger
CEO

An Open Letter to an Open Ecosystem (2021)

Community & Policy Advocacy

Intel partners with a range of industry-leading organizations, academic, and governance bodies to accelerate our shared secure, data-centric vision.

Technology Vendor Partnerships

Intel spearheads a cross-industry council with 20+ industry-influencing companies to accelerate our collective understanding of the latest security threats, validate potential impacts, develop mitigations, and coordinate vulnerability disclosures.

Industry Initiatives

Intel is active in initiatives that focus on data security and privacy. Intel contributes to numerous industry consortiums, with an emphasis on developing industry-wide standards for technology, security assurance, and development.

Policy and Government

Intel advises policymakers and governments on strategies to advance product security through regulatory compliance, external advocacy, and supply chain best practices. We also advocate for public-private partnerships and policies that support scalable, global standards.

Academic Investment and Partnerships

Intel believes collaboration through academic investments and partnerships is critical to fueling innovation. Our relationships with leading security research institutions allow us to work with top talent worldwide.

Collaboration with Industry

Intel is active in industry initiatives focused on data security and privacy, emphasizing developing technology, security assurance, and development standards.

Industry Initiatives

Technology Standards

Intel leads and participates in industry consortiums and standard bodies shaping how technologies should be designed to meet security, privacy, and safety requirements.

Examples include:

- Trusted Computing Group (TCG)
- Confidential Computing Consortium (CCC)
- 3rd Generation Partnership Project (3GPP)
- National Institute of Standards and Technology (NIST)
- International Organization for Standardization (ISO)

Product Design, Assurance and Risk Management Standards

Intel is driving secure-by-design best practices, systemic mitigations, automated vulnerability scanning tools, and hardware security training, among other efforts.

Examples include:

- MITRE: Collaborating to extend Common Weakness Enumeration (CWE) to include 75 hardware weaknesses
- Involvement in Common Vulnerabilities and Exposures (CVE) and Common Attack Pattern Enumeration and Classification (CAPEC)
- Forum of Incident Response and Security Teams (FIRST) focused on Common Vulnerability Scoring System (CVSS) and Product Security and Incidence Response (PSIRT)

Domain-Specific Design and Verification Standards

Intel drives know-how and capabilities into domain-specific product design, development, operation, and manufacturing processes.

Examples include:

- Accellera System Initiative
- SEMI
- Open Source Security Foundation (OpenSSF)
- Unified Extensible Firmware Interface (UEFI) Forum

Back to Table of Contents

CVE Data

This section details information about Intel's remediation of security vulnerabilities in 2022 as well as provides historical context and data.

Proactive Vulnerability Discovery, a Competitive Advantage

Intel's **Jerry Bryant** and **Christopher (CRob) Robinson** on the 2022 Intel Product Security Report CVE data

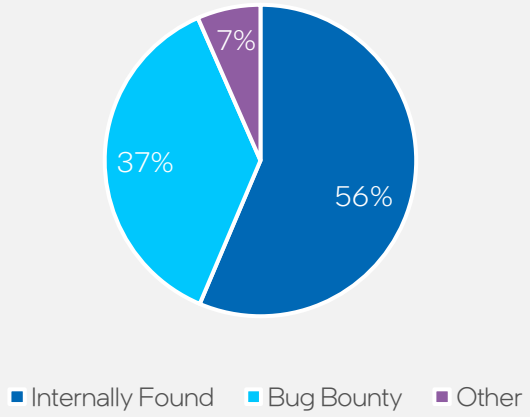
InTechnology **Video:** CVE and Risk Management with Katie Noble

Impact of Intel's Investment in Product Security Assurance

Customers say they prefer vendors who proactively find, mitigate, and communicate security vulnerabilities*. While the majority of potential vulnerabilities are found and mitigated in the product development process, our Security-First pledge drives our commitment to finding and mitigating issues long after products ship.

In 2022, 93% of issues addressed resulted from Intel's proactive product security assurance investments. In addition, internal security research accounted for 56% of the issues addressed, while 37% were reported through Intel's Bug Bounty program.

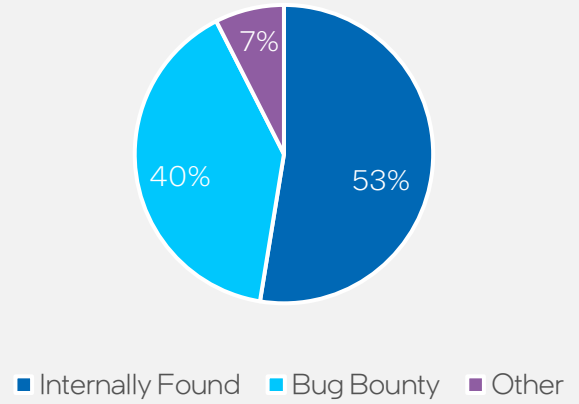
Intel's investment accounts for 93% of vulnerabilities addressed in 2022



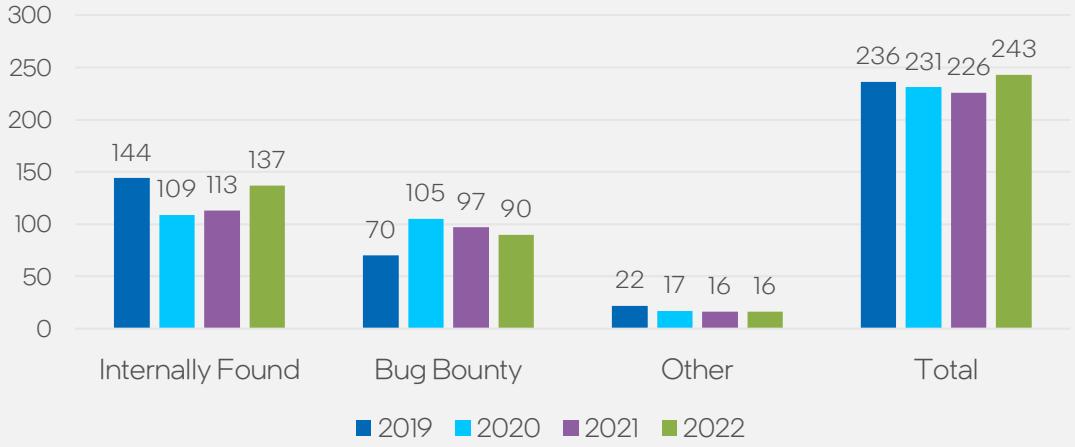
*Intel Study: Transparency and Security Assurance Drive Preference

As the last four years of product security report data shows, Intel proactively found and mitigated 93% of the vulnerabilities addressed as part of our investment in product security assurance.

2019 - 2022, 93% of issues attributed to Intel's proactive investment in product security assurance



2019 - 2022 Comparison

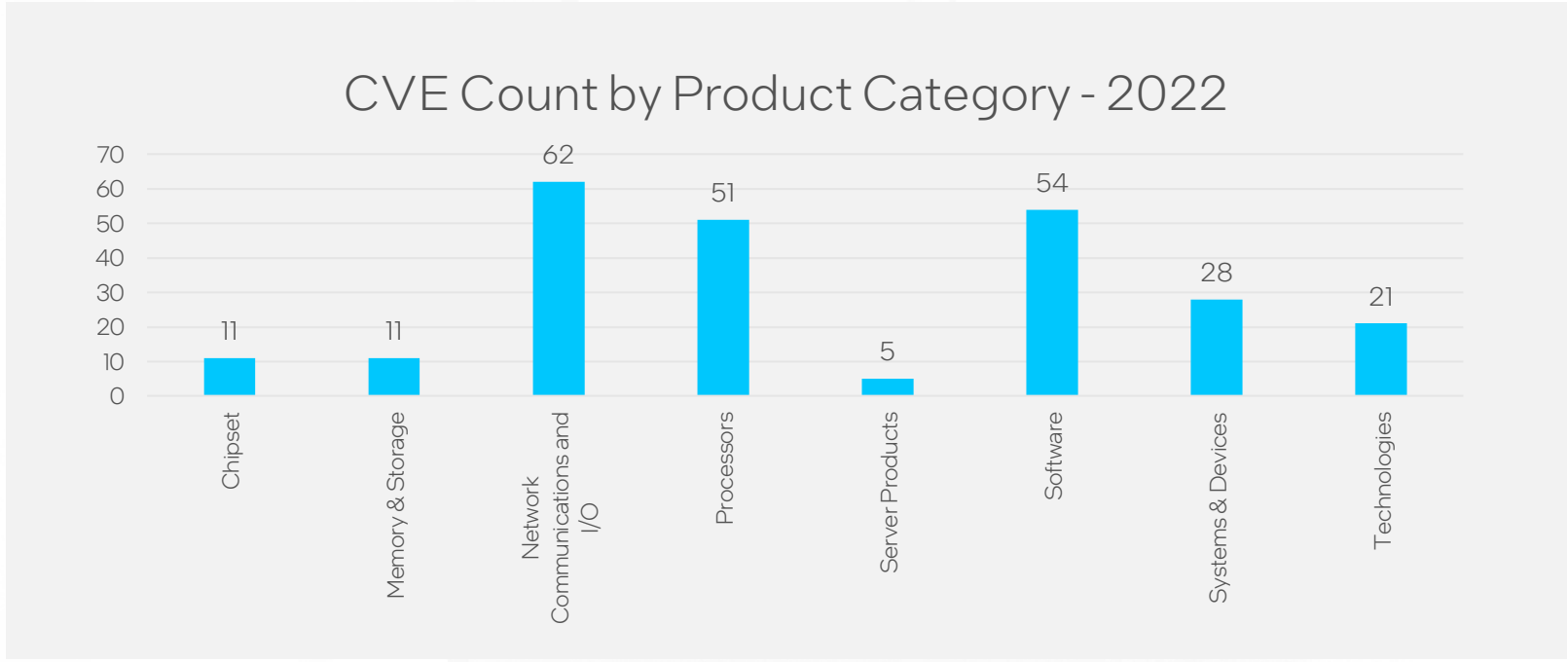


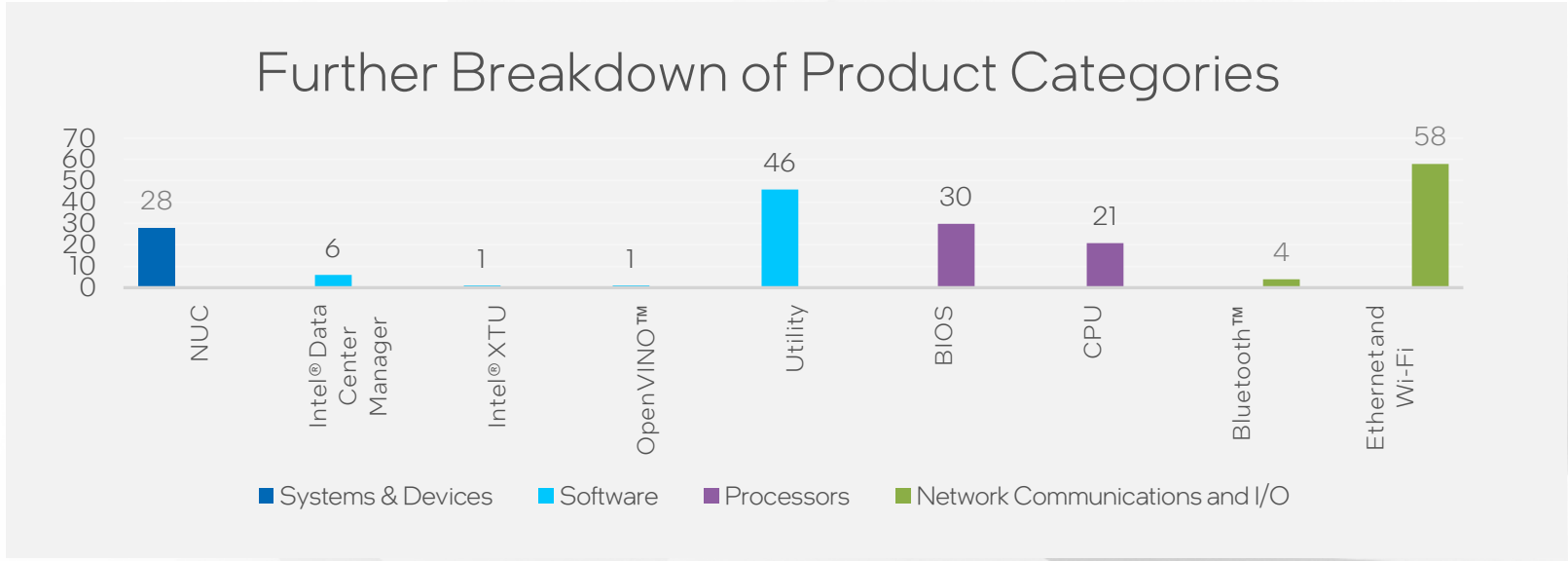
CVEs by Product Category

With Intel's vast portfolio of products, including hardware, software, and services, it is important to analyze data by product category to help identify areas of potential focus for developing systemic mitigations, education, and tooling that help to eliminate future escapes during product development.

In chart 2, we break down the top 4 product categories into sub-categories to further identify where issues originated.

Note: the "Utility" category represents various software applications from Intel.



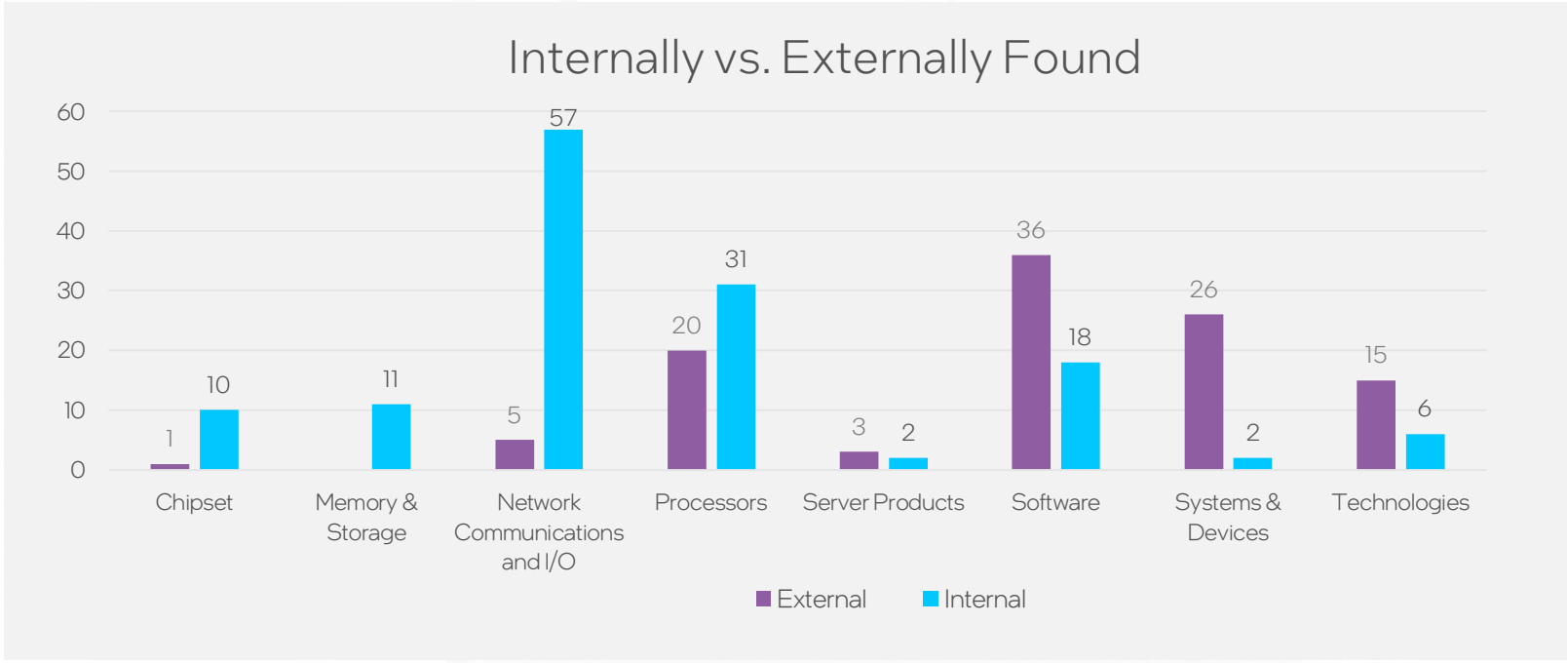


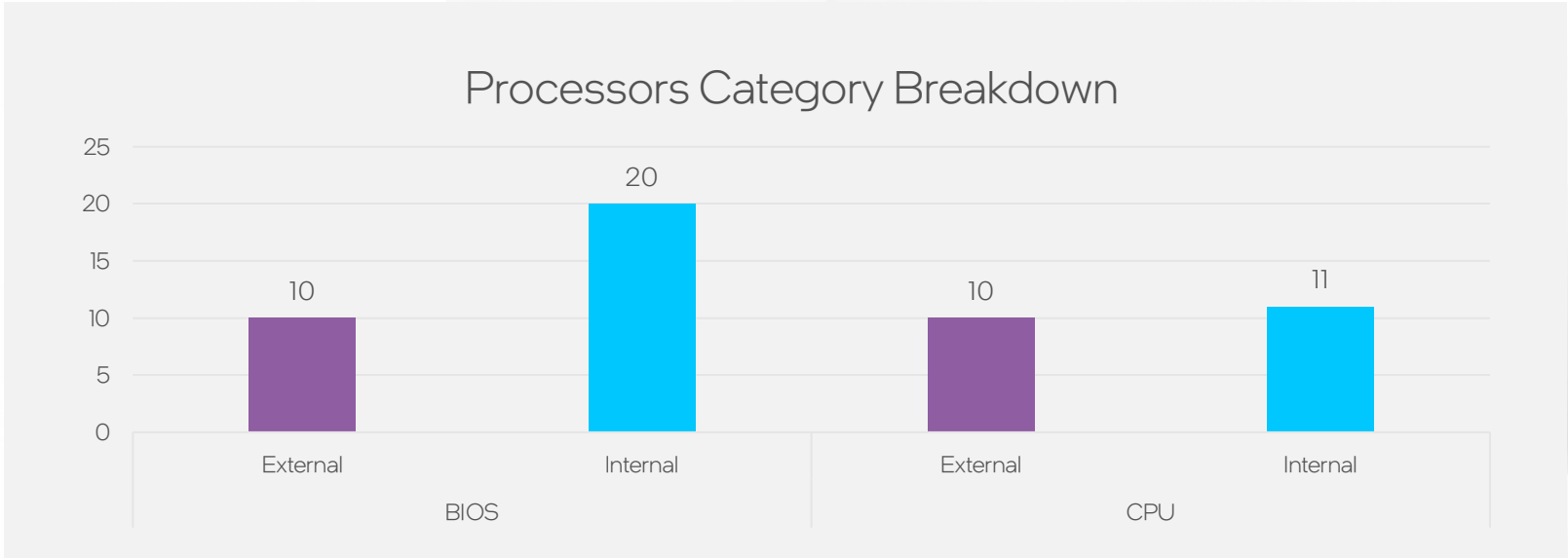
CVEs by Product Category – Internally/ Externally Found

The scale of Intel's security capabilities is unmatched. To deliver security at scale, we have over 500 dedicated product security staff, perform over 120 hackathons per year, fund 40+ academic research teams, and continue to expand our Bug Bounty programs in innovative ways.

In 2022, Intel found 56% of the vulnerabilities addressed internally, and 37% were reported through our Bug Bounty programs. The remaining 7% came from various sources, such as open source projects managed by Intel and organizations that do not or cannot seek bug bounty payments.

We continue to deliver on our Security-First Pledge through investment, maturity of process, community engagement, and transparency in reporting results.





CVE Severity

2022 severity stats:

- 7% of vulnerabilities were rated low severity
- 58% of vulnerabilities were rated medium severity
- 33% of vulnerabilities were rated high severity
- 2% of vulnerabilities were rated critical severity

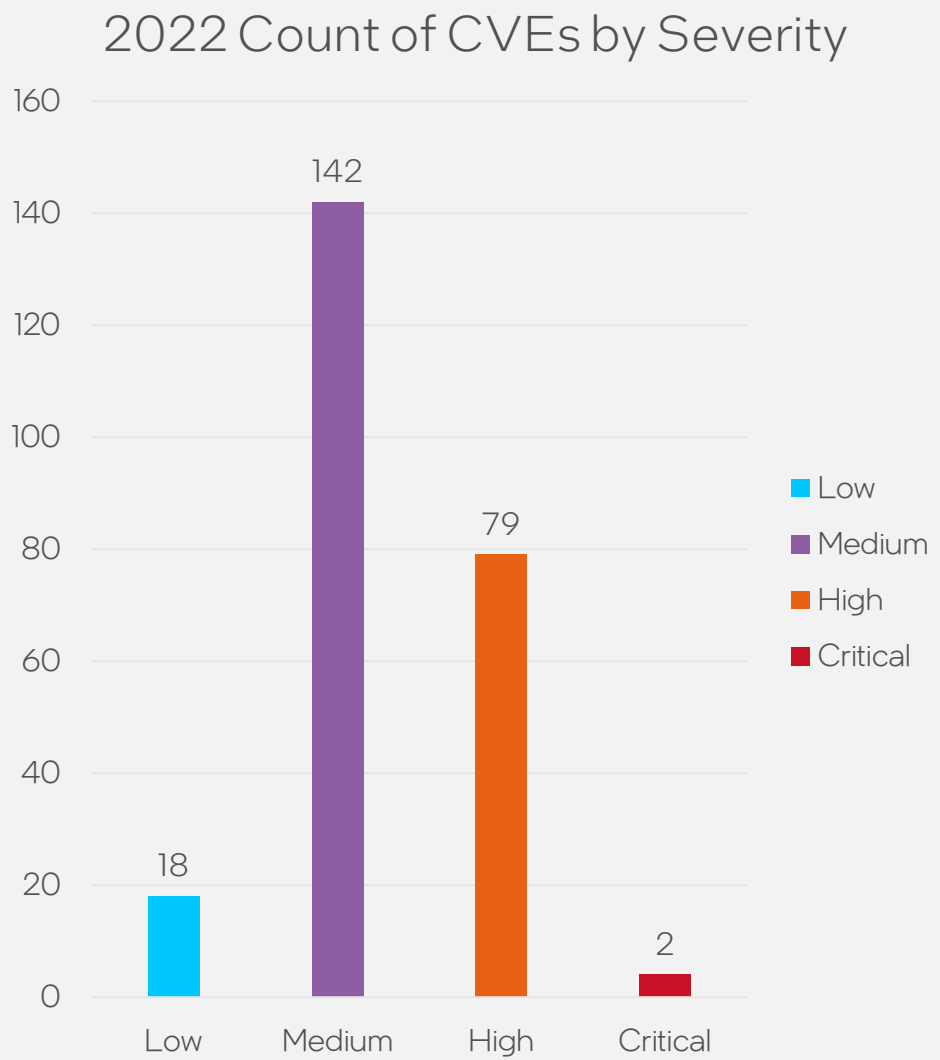
The Common Vulnerability Scoring System is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental.

The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments. The Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability unique to a user's environment. The Base metrics produce a score ranging from 0 to 10, which can be modified by scoring the Temporal and Environmental metrics.

The impact of most medium, high, and critical vulnerabilities is the potential elevation of privilege. In the case of medium-severity issues, these mostly require an authenticated user on the same physical network or who has physical or local access to a vulnerable system. These issues become high or critical if an unauthenticated user can trigger the vulnerability and/or reach a vulnerable system from outside the local area network.

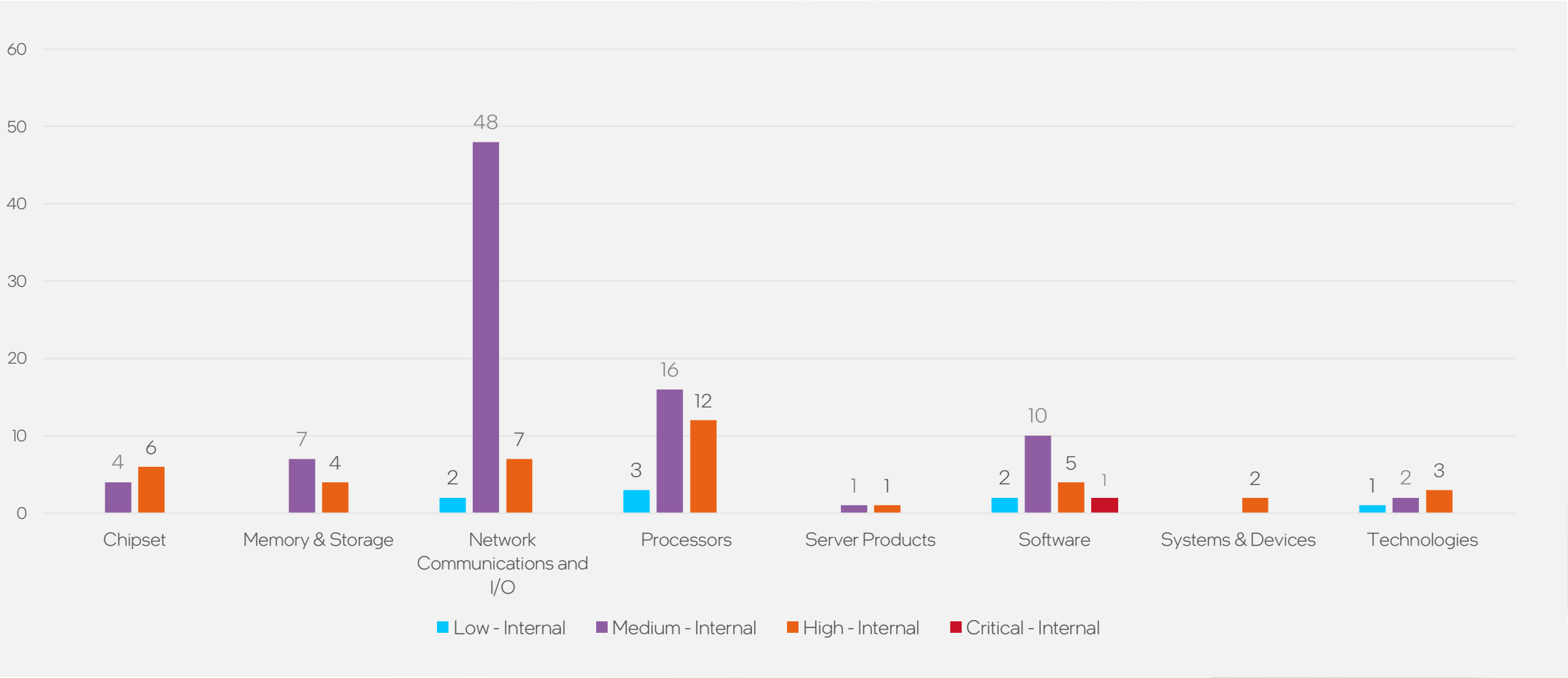
CVSS severity scores fall into five categories

None:	0.0
Low:	0.1–3.9
Medium:	4.9–6.9
High:	7.0–8.9
Critical:	9.0–10.0



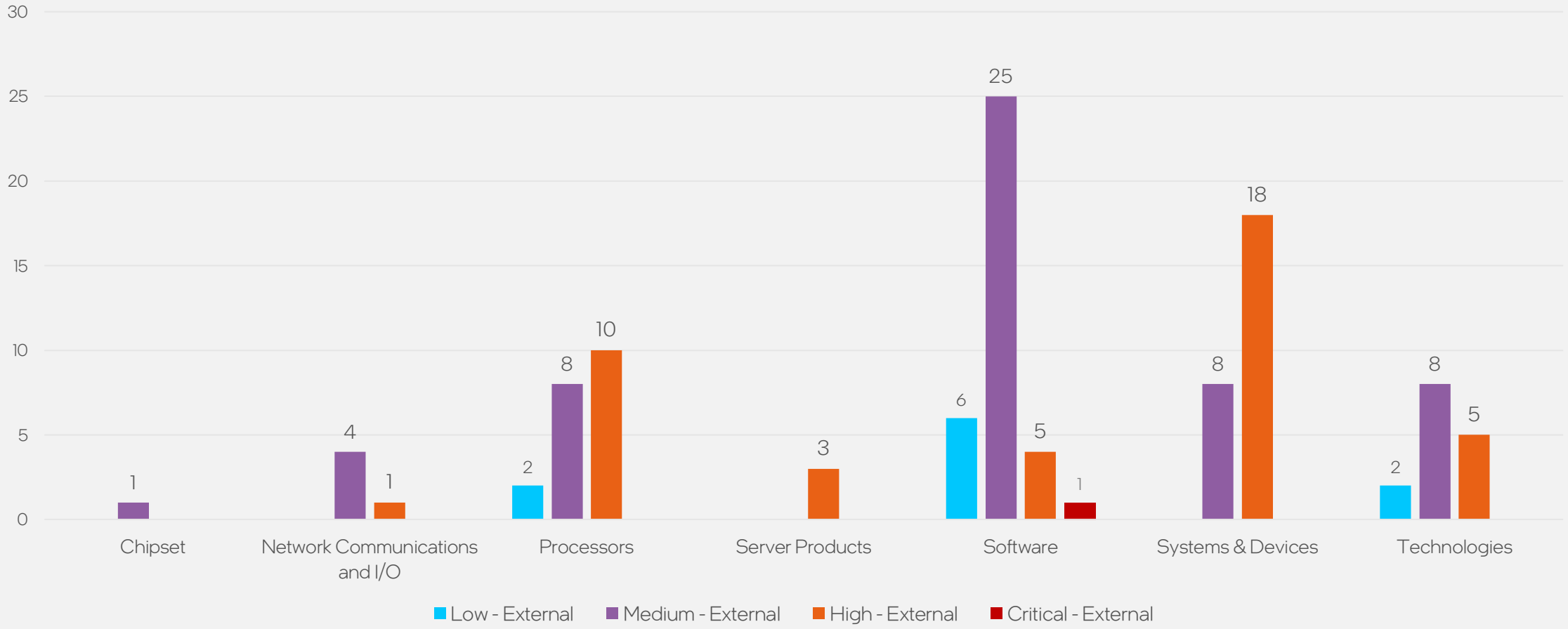
Severity of Internally Found by Product Category

As part of Intel's commitment to transparency, these issues were assigned CVE IDs and publicly reported via an industry-standard security advisory on https://intel.com/security.



Severity of Externally Found by Product Category

Of the 106 vulnerabilities reported by external researchers, 90 (85%) were reported through Intel's Bug Bounty Program. The majority of external research in 2022 focused on the Software and the Systems & Devices categories.



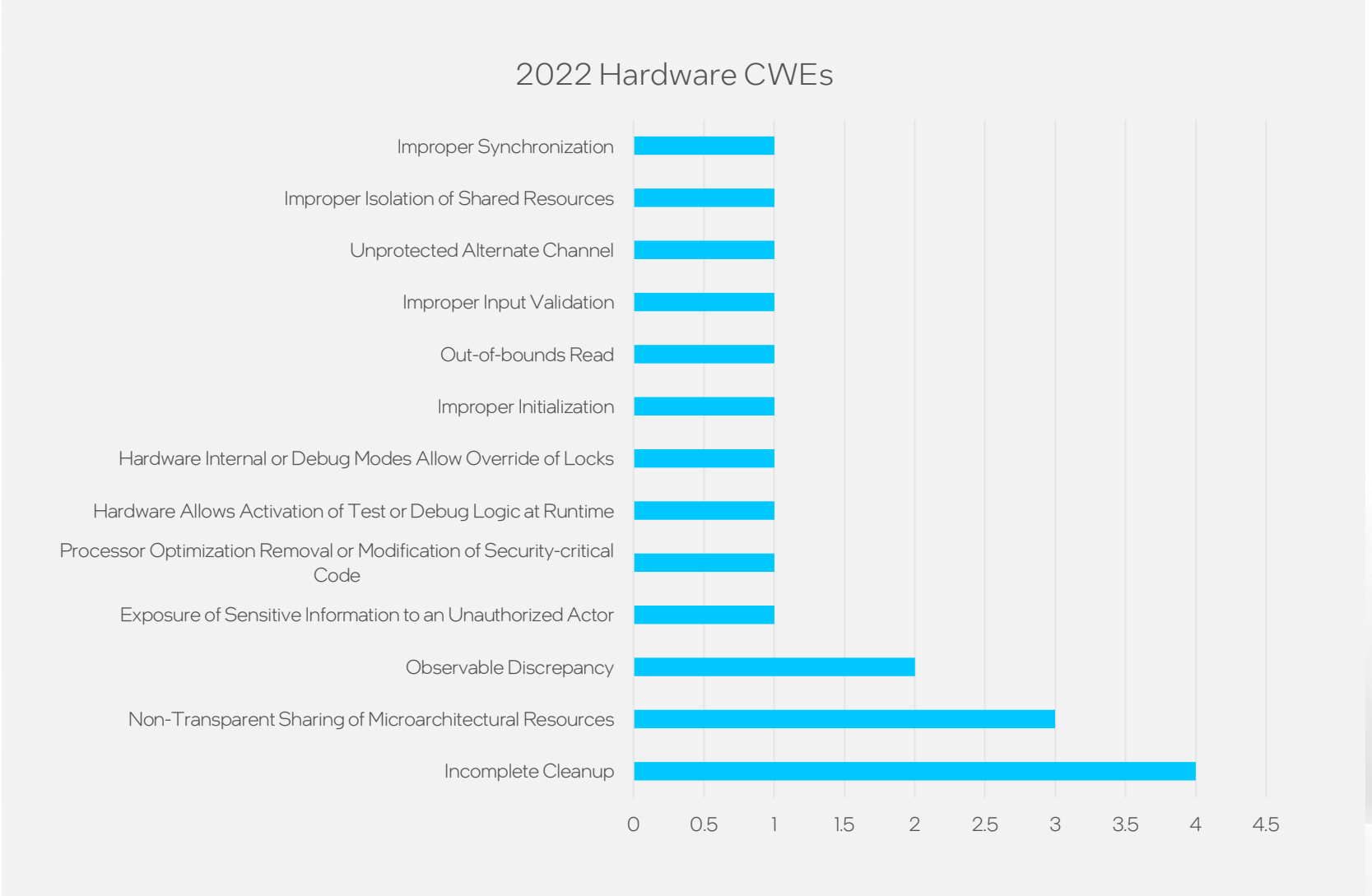
Hardware Common Weakness Enumeration (CWE) Data

In 2021, Intel helped to drive the creation of the hardware Common Weakness Enumeration (CWE) now used across the industry along with software CWEs.

2022 represents the first full year of hardware CWE implementation at Intel. All weaknesses identified in product development or after products ship, are tracked and analyzed as part of Intel's SDL program to help direct attention to specific areas that may benefit from systemic mitigations, education, and/or tooling to help eliminate these weaknesses in product development.

The chart shows 13 hardware CWEs that were assigned to the 19 hardware vulnerabilities addressed in 2022.

Intel's **Jason Fung** talks about collaborating with the industry to create hardware CWEs



Back to Table of Contents

Reference

Intel.com Product Categories

Processors
Intel® Xeon® Scalable
Intel® Xeon®
Intel® Core™
Pentium®
Celeron®
Intel Atom®
Intel® Movidius™ VPUs
IoT and Embedded Processors

Systems & Devices Intel® Evo™
Laptops
Intel® NUC
Desktops
Workstations
Intel vPro®

Server Products
Single Node Servers
Multi Node Servers
Intel® Data Center Systems
Server Chassis
Server Boards
SAS/RAID Products
Intel® Server Management

FPGAs & Programmable Devices
Intel® FPGAs, CPLDs, and Configuration Devices
Intel® Quartus® Prime Design Software
Intellectual Property
Intel FPGA Development Kits
Acceleration Boards & Platforms

ASICs
Intel® eASIC™ Devices
Intel® Blockscale™ ASIC

Chipsets
Mobile
Desktop
Server
Embedded

Graphics Processing Units
Intel® Arc™
Intel® Iris® Xᵉ MAX
Intel® Data Center GPU Flex Series

Memory & Storage Solid State Drives
Intel® Optane™ Persistent Memory
Datacenter Storage Solutions

Wireless Products
Intel® Killer™ Wireless Products
Intel® Wi-Fi 6E Products
Intel® Wi-Fi 6 Products
Intel® Wireless-AC Products
Intel Mobile Broadband Solutions

Network Communications and I/O
Intel® Ethernet Technologies
Intel® Ethernet Products
Intel® Infrastructure Processing Unit (Intel® IPU)
Intel® Silicon Photonics Optical Transceivers
Programmable Ethernet Switch Products
Thunderbolt™ Technology

Links

Intel Security First Pledge

Security Development Lifecycle (SDL)

Intel Advanced Security Development Practices

Software Security Guidance

Intel Platform Update

Chips & Salsa Podcast

InTechnology Podcast

Security Research

Vulnerability Management

Coordinated Vulnerability Disclosure

Product Security Center

Industry Engagement

Intel Security Blog

Intel Bug Bounty Program

Project Circuit Breaker

Study: Transparency and Security Assurance Drive Preference

Academic Research and Community Outreach

Introduction to Intel Transparent Supply Chain on Lenovo ThinkSystem Servers

intel security

Notices & Disclaimers

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.