IOActive®
Research-fueled Security Services

Introduction & Importance of OCP S.A.F.E.
Securing Tomorrow's Technology Today

What is OCP?

The Open Compute Project (OCP) is a consortium of organizations dedicated to fostering innovation and collaboration in the digital infrastructure and supply chain space. These organizations, including IOActive, which is an approved OCP Security Review Provider (SRP), drive forward new technological standards and strategic initiatives designed to enhance security, reduce complexity, and streamline the development process.

What is OCP S.A.F.E.?

The Open Compute Project Security Assessment Framework and Execution (OCP S.A.F.E.) is a newly published set of guidelines aimed at enhancing the security of device firmware and hardware in cloud computing environments. This framework is critical for ensuring that all production versions of device firmware are rigorously assessed for vulnerabilities and potential threats. OCP S.A.F.E. assessments also provide security assurance for organizations regarding the hardware and components intrinsic to their production processes, business operations, and supply chains.

Why It Matters

OCP S.A.F.E. was established to combat the security challenges organizations face today. Organizations must maintain operational effectiveness in the face of increasingly sophisticated cyber threats, and while the globalization of the supply chain has provided countless opportunities for business growth, this expansion has also created a broader attack surface.

Unfortunately, threat actors will target the weakest link in a supply chain and this may include suppliers, third-party vendors, software, and even the hardware and components supporting production lines.

Compliance with OCP S.A.F.E. is now a strategic imperative for securing data centers and cloud services. The framework provides the most effective approach to minimizing risk and reducing cyber threat exposure across the entire supply chain. Furthermore, OCP S.A.F.E. standards provide security and quality assurance for device manufacturers and vendors, while establishing a level of trust that extends to the end user.

Leading the Way in OCP S.A.F.E. Compliance

Pioneering Role: IOActive has been at the forefront of the OCP S.A.F.E. initiative from its inception. Our own CTO, Gunter Ollmann, a notable figure in cybersecurity, played a critical role in starting this project during his tenure at Microsoft, and was a part of the original OCP S.A.F.E. group. Furthermore, IOActive's Director of Secure Engineering, Ivan Reedman, is the driving force and co-creator of the OCP S.A.F.E. SRP Requirements documentation, which provides a guideline for SRP organizations to conduct quality assessments of software, hardware, and firmware designs in line with industry practices.

This deep-rooted involvement gives us unmatched insight and influence in shaping the standards.

Defining Technical Methodology: The technical backbone of OCP S.A.F.E. continues to be updated by members of the IOActive team. This leadership in defining the methodologies not only establishes IOActive as a key player but also ensures that we are at the cutting edge of security methodology development.

Trusted Security Review Partner (SRP): As a founding provider, IOActive is recognized for its integrity as a trusted OCP S.A.F.E. Security Review Partner. This trust is built on our consistent delivery of quality assessments and our foundational role in creating the OCP S.A.F.E. SRP requirements. Major cloud computing companies, which are long term clients, rely on OCP S.A.F.E. reports generated by IOActive to establish a high degree of trust and security assurance with vendors and end users.

Continual Advancement: IOActive doesn't just apply OCP S.A.F.E. standards; we help drive their evolution. Our ongoing work assessing the Caliptra open-source artifact—developed by Microsoft and Google for hardware vendors—underscores our pivotal role in advancing industry security practices. This involvement also reflects our adaptability and commitment to leveraging the latest tools to benefit our clients. Caliptra is an open source root of trust project that was founded by AMD, Google, Microsoft and NVIDIA.

Caliptra on GitHub

IOActive OCP S.A.F.E. SRP of Choice

- Co-creators of the OCP S.A.F.E. methodology
- Regular partners to Global Cloud Computing Platforms
- Continuously driving advancements in security standards
- Almost two decades as a trusted authority in advanced hardware and sophisticated embedded devices

IOActive's OCP S.A.F.E. Services & Methodology

Our Services

IOActive prides itself on straightforward and effective security testing, threat modeling, and code auditing.

As an SRP, IOActive has a comprehensive understanding of the full Secure Development Lifecycle (SDL) and we assist clients during each stage of the OCP S.A.F.E. integration process.

During each step of the OCP S.A.F.E. process, we provide our clients with detailed assessments, documentation and recommendations helping our customers achieve OCP S.A.F.E. certification.

IOActive delivers a comprehensive suite of services tailored to meet the OCP S.A.F.E. standards:

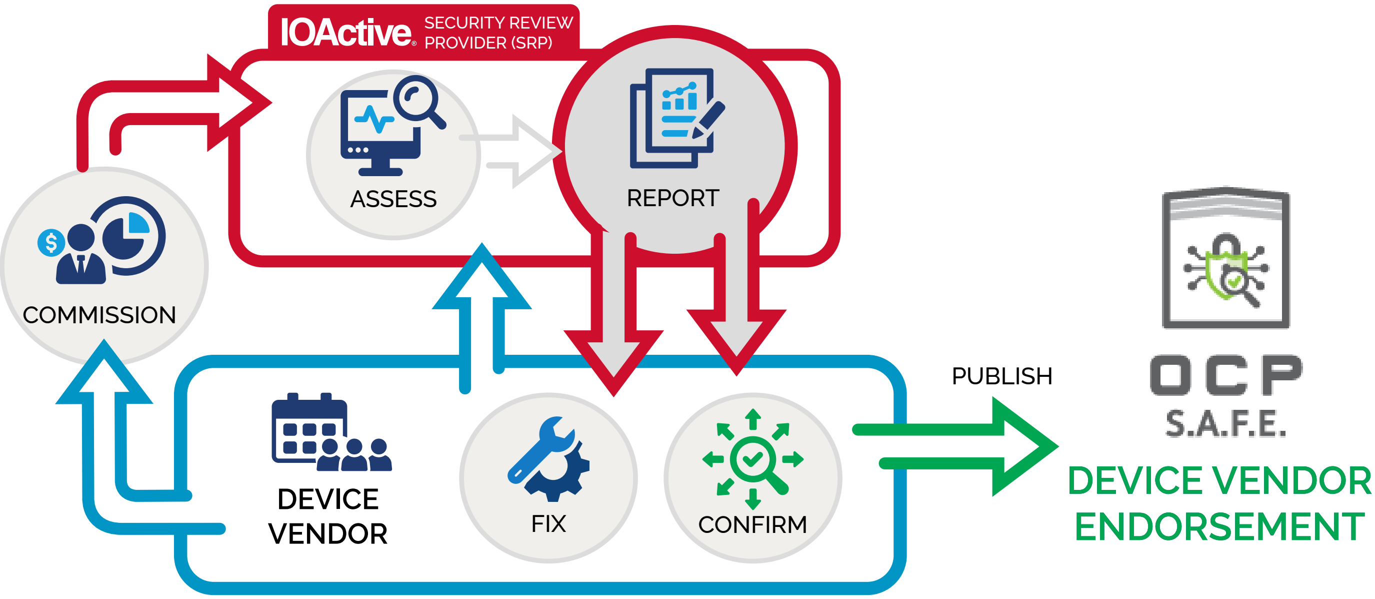
- **Scope 1:** Document Analysis, Code Review and Build Environment: This scope broadly covers privileged software and firmware in the context of a single device or function. Areas of emphasis include document analysis, code review, and a review of the build environment.
- **Scope 2:** Focusing on Trusted Execution Environments (TEEs): This scope focuses on how TEE trust boundaries are handled and compliance with TEE standards. Examples include devices with root of trust and security processors for SOC management, and host capabilities such as SGX, TDX, SEV, and Trustzone for user or application isolation and protection.
- **Scope 3:** Resilience to physical attacks: This scope is intended to cover devices and systems that require assessing their resilience to physical attack. Parts of a system-on-chip (SoC) that may require this level of analysis include root of trust, security processor, logic handling, long term secrets, and crypto accelerator blocks. Ideally, an RTL review should be performed to determine if the necessary design mitigations are in place in addition to physical side channel analysis and fault injection.

- **Reports:**
  - A confidential Final Report will be provided at the end of the engagement, with a meeting to review details and answer questions.
  - A digitally-signed short form report for publishing with cloud providers and OCP S.A.F.E.
  - See our public report on Threat Modeling for SK hynix

Methodology in Action

Our approach combines rigorous analysis with real-world applicability. We apply the fundamental principles of OCP S.A.F.E. as a framework rather than a quickly outdated prescriptive and restrictive checklist.

OCP S.A.F.E. SRP Commissioned Security Review Process


IOActive SECURITY REVIEW PROVIDER (SRP)
COMMISSION
ASSESS
REPORT
DEVICE VENDOR
FIX
CONFIRM
PUBLISH
OCP S.A.F.E.
DEVICE VENDOR ENDORSEMENT

Continuous Engagement Model

An OCP S.A.F.E. security review is not a one-time event but an ongoing process. Our OCP S.A.F.E. engagements are designed to evolve with your needs and the changing landscape, ensuring ongoing protection and compliance:

- **Iterative Assessments:** We conduct full and incremental assessments to address both comprehensive security evaluations and targeted reviews of vulnerability fixes or feature enhancements.
- **Remediation and Follow-Up:** After initial assessments, we provide detailed remediation guidance and perform follow-up evaluations to ensure all security measures are effectively implemented and maintained.
- **Long-term Partnership:** We work closely with our clients as a strategic partner to help them develop a secure product development lifecycle, leveraging security practices in line with the latest industry developments and compliance requirements.

Keep Your Proprietary Technologies Secure With IOActive

IOActive's OCP S.A.F.E. methodologies balance the need for robust security and the protection of your intellectual property. By following OCP S.A.F.E. guidelines, we can examine and test proprietary technologies to meet security assurance and OCP S.A.F.E. adopter requirements without exposing or sharing proprietary technologies.

IOActive understands how crucial it is to secure proprietary technologies, and we have a track record of maintaining the confidentiality of valuable intellectual property, including source code.

IOActive

Why Choose IOActive

Unmatched Expertise

With almost three decades of security ground-breaking research and active involvement in setting industry standards, IOActive is recognized globally for its deep security expertise and innovative approach. Our team is composed of world-renowned security researchers and consultants who bring a proactive, attacker-minded perspective to every project.

Client-Centric Security Solutions

We understand that each client has unique security needs and business objectives. At IOActive, we tailor our services to align with your specific goals, providing customized security solutions that protect your key assets while maintaining operational effectiveness.

For more information about IOActive's Cybersecurity Services, email info@ioactive.com or visit ioactive.com.

Prepare for the Future Now

Companies trust IOActive because:

1. **Pioneering Research:** Renowned for ground-breaking cybersecurity research, uncovering vulnerabilities that shape industry standards.
2. **Expert Cybersecurity Assessments:** Drawing on extensive expertise, we uncover risks often overlooked by others, ensuring robust protection for your infrastructure.
3. **Customized Advice:** We deliver personalized cybersecurity strategies that address our client's specific business needs and threats.
4. **Global Industry Recognition:** Acknowledged by both peers and clients, our contributions to the cybersecurity community have earned a prestigious reputation.
5. **Innovative Cybersecurity Tools:** Leveraging state-of-the-art tools and techniques, we are at the forefront of cybersecurity technology.
6. **Dedicated Client Partnership:** We prioritize long-term client relationships, offering continuous support and strategic guidance to navigate the evolving security threatscape.

ABOUT IOACTIVE

IOActive, a trusted partner for Global 1000 enterprises, provides research-fueled security services across all industries. Our cutting-edge cybersecurity teams provide highly specialized technical and programmatic services including full-stack penetration testing, program efficacy assessments, and hardware hacking. IOActive brings a unique attacker's perspective to every engagement to maximize cybersecurity investments and improve the security posture and operational resiliency of our clients. Founded in 1998, IOActive is headquartered in Seattle with global operations, including state of the art hardware hacking labs in Seattle, WA, Madrid, Spain and Cheltenham, UK. For more information, visit ioactive.com.