IOActive®

Research-fueled Security Services

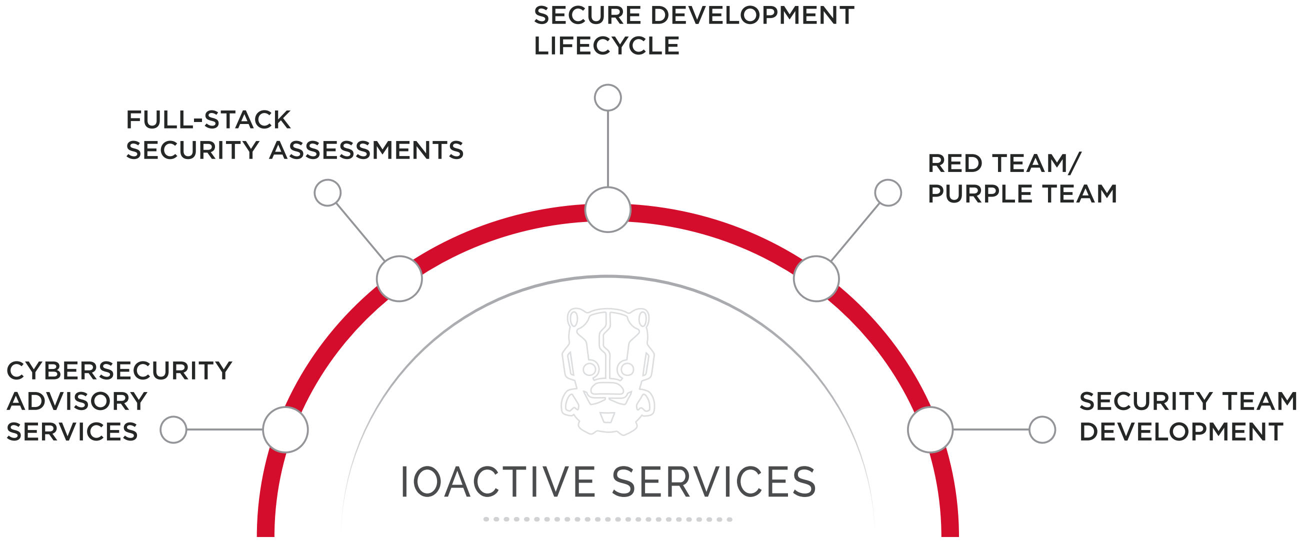
SECURITY SERVICES FOR YOUR BUSINESS, SITUATION, AND RISKS

For more than two decades, IOActive has delivered research-fueled security services to many of the world's leading companies. We meld an attacker's perspective with an understanding of your risk profile to uncover high-risk weaknesses wherever they reside in your environments and products. We transfer knowledge and deliver actionable, vendor-agnostic recommendations that empower organizations to stay ahead of threats and measurably improve business resiliency.

Our game-changing approach, using time-tested techniques aligned to your business, is a key reason why we've been recognized as one of the most important security companies in the last 30 years. And why enterprises and product manufacturers across a wide range of industries trust us to help them grow and innovate securely.

AT A GLANCE

- Pure-play, global security services provider
- Attacker's perspective to assessing operational resiliency
- Depth and breadth of services across the full stack, paired with industry expertise
- Research-fueled knowledge transfer
- Vendor-agnostic, actionable recommendations



SECURE DEVELOPMENT LIFECYCLE

FULL-STACK SECURITY ASSESSMENTS

RED TEAM/ PURPLE TEAM

CYBERSECURITY ADVISORY SERVICES

SECURITY TEAM DEVELOPMENT

IOACTIVE SERVICES

CYBERSECURITY ADVISORY SERVICES

IOActive has unique expertise in both the technical and the strategic advisory realms. Many firms handle one or the other. We provide both because that's what's required to build real resilience to increasingly complex cybersecurity risks. We've learned that a merely technical fix is of limited value if a company's overall operations are riddled with vulnerabilities.

- Through our advisory work, we give clients programmatic assistance in uncovering latent risks in IT, Operational Technology (OT), and Product Technology (PT) environments.
- Our advisory services include an extensive suite of offerings to meet your specific needs—including enterprise data-security mapping and threat-scenario analysis.
- We ask the right questions to help you define your unique programmatic security requirements and walk you through a systematic review of your organization's particular risks.

> *"We work on more layers of the technology stack, and provide more security services offerings across more environments than any other firm today, so we can meet our clients where they are to deliver game-changing recommendations and value."*
>
> John Sheehy
> SVP, Research and Strategy, IOActive

FULL-STACK SECURITY ASSESSMENTS

Most security companies only scan for threats at the network or application level. IOActive is the only global provider that looks at your entire system. We pioneered Full Stack Security assessments to identify potential gaps throughout a client's environment without disrupting existing operations. We drill all the way down to the facility and semiconductor level; we go all the way up to strategic impacts of personnel, process, and supply-chain security. We also carefully assess every layer in between.

- Our assessment of all levels of the technology stack makes IOActive a true "one-stop-shop" for high-end cybersecurity expertise – the only one of its kind in the industry.
- Most companies' current protection strategies rely on end-point security. Our layered security strategy provides increased protection at points of IT-OT-PT convergence to increase the difficulty of exploitation, using compensating controls when needed to mitigate operational impact.
- At higher levels of the stack, we assess a wide range of strategic elements, including programs, policies, and governance.

SECURE DEVELOPMENT LIFECYCLE

Products of all kinds are increasingly vulnerable to sophisticated breaches as more of their intellectual property shifts to the silicon layer. We understand the unique vulnerabilities of the development and deployment cycle—and how those vulnerabilities differ across myriad forms of software, hardware, and integrated products. Our own cutting-edge research labs in the Americas and EMEA uniquely position us to help clients identify product technology threats anywhere throughout their development, production and supply chains and embed "security by design."

- For clients with dynamic product and service portfolios, we provide lifecycle-security advice, as well as the independent validation and verification that is central to a mature SDL.
- IOActive has long been a pioneer in product cybersecurity. We virtually created the vehicle-cybersecurity market with our original research on the cybersecurity risks of connected vehicles such as the Toyota Prius, Ford Escape, and Jeep Cherokee.
- In addition, IOActive has been the first to identify important vulnerabilities across a range of systems, including smart meters, commercial-satellite terminals, traffic-control equipment, in-flight entertainment communications (IFEC), and various medical devices. We move that knowledge quickly into our services offerings.

RED TEAM/PURPLE TEAM SERVICES

We help your organization develop a clear understanding of cyber threats from the perspective of attackers—not compliance auditors. We go beyond standard penetration testing, and provide full adversary emulation, comprehensively simulating the specific threats to your organization, so you can learn the truth about your operational resiliency.

- Regulatory compliance, while important, is not the same thing as real-world security. Our objective is to help you focus on effective security. That is what our red-team and purple-team procedures are designed to achieve.
- We can either provide or advise on the creation of continuous, independent, and real-world attacker-emulation services that work with a "blue team"—your own security-operations personnel—to prepare them to face the adversaries your enterprise is likeliest to encounter.
- Our original research and breach analysis give us detailed insight into how hackers have penetrated organizations across a diverse range of sectors and circumstances. Our emulation and testing services bring this insight to bear on your behalf.

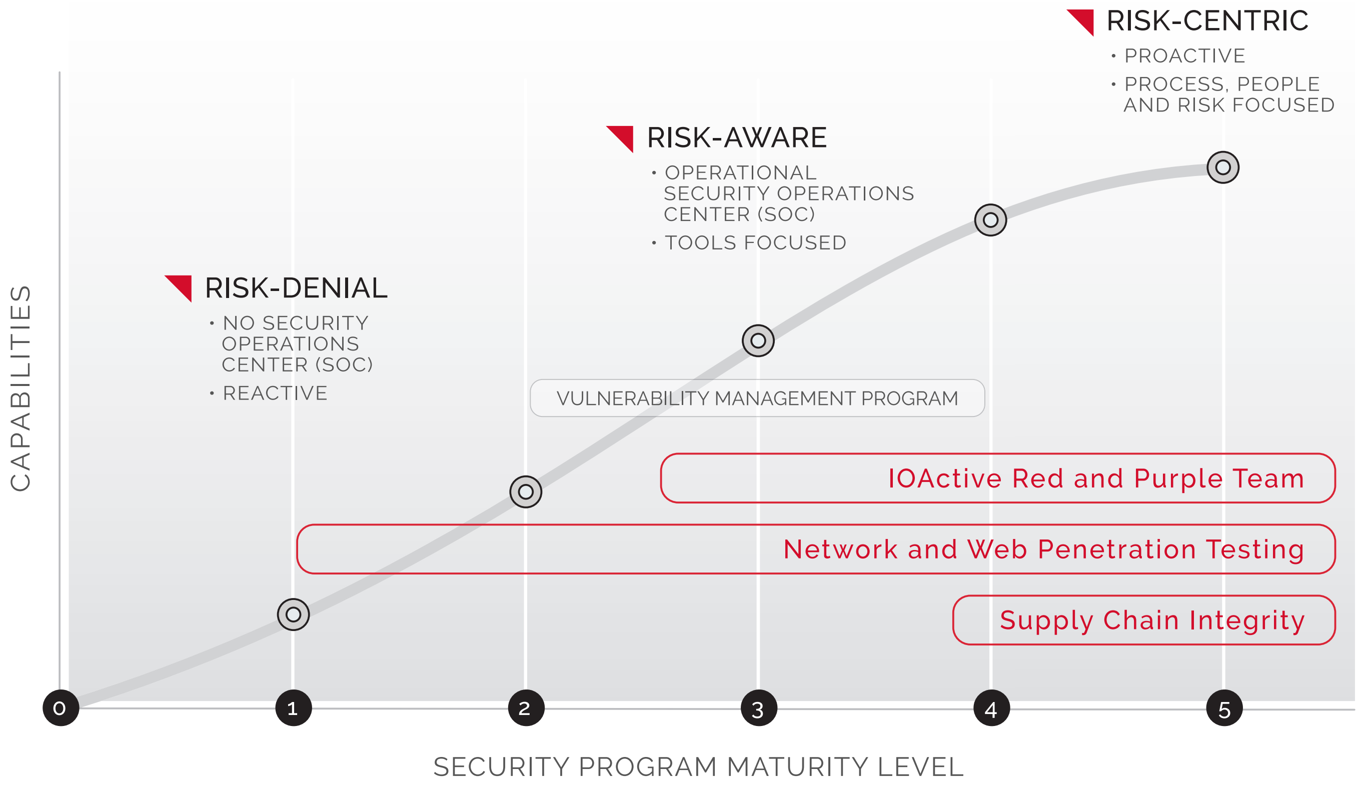
> *With our breadth and depth of services offerings across more environments than any other firm today, we can deliver specific, high-value recommendations based on your business, unique situation, and the risk you face.*

SECURITY TEAM DEVELOPMENT

Our primary aim is to empower your organization to protect itself against cybersecurity threats.

The best way to do that is to consistently invest in an in-house team that has the capabilities and the awareness it needs to safeguard your operations against an ever-evolving threatscape. We know how to build a world-class cybersecurity team capable of staying ahead of adversaries—and we want to transfer that knowledge to you to help protect your interests.

- Too many organizations are highly reactive in their cybersecurity posture. By strengthening your cybersecurity team's ability to anticipate and proactively address threats, you will put yourself ahead of the danger and ahead of many—if not all—of your competitors.
- Team development is central to any comprehensive "secure-by-design" cybersecurity strategy—the approach best suited to today's complex threatscape and long component lifecycles.
- Like all of IOActive's services, our team development work is carefully customized to the unique needs of your company and your industry. The most sophisticated cybersecurity threat actors pay close heed to the distinctive patterns of your firm and your sector—your cybersecurity protection should do no less.


RISK-CENTRIC
• PROACTIVE
• PROCESS, PEOPLE AND RISK FOCUSED
RISK-AWARE
• OPERATIONAL SECURITY OPERATIONS CENTER (SOC)
• TOOLS FOCUSED
RISK-DENIAL
• NO SECURITY OPERATIONS CENTER (SOC)
• REACTIVE
VULNERABILITY MANAGEMENT PROGRAM
IOActive Red and Purple Team
Network and Web Penetration Testing
Supply Chain Integrity
CAPABILITIES
0
1
2
3
4
5
SECURITY PROGRAM MATURITY LEVEL

SC MEDIA AWARDS 30th Anniversary

One of the **Most Important Cybersecurity Companies** of the Last 30 years

2 of 3 **Most Important Researchers** of the Last 30 years

REBOOT 19 SC Media Reboot Leadership Awards

ABOUT IOACTIVE

IOActive is a trusted partner for Global 1000 enterprises, providing research-fueled security services across all industries. Our cutting-edge security 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 client engagement to maximize security investments and improve clients' overall security posture and business resiliency.