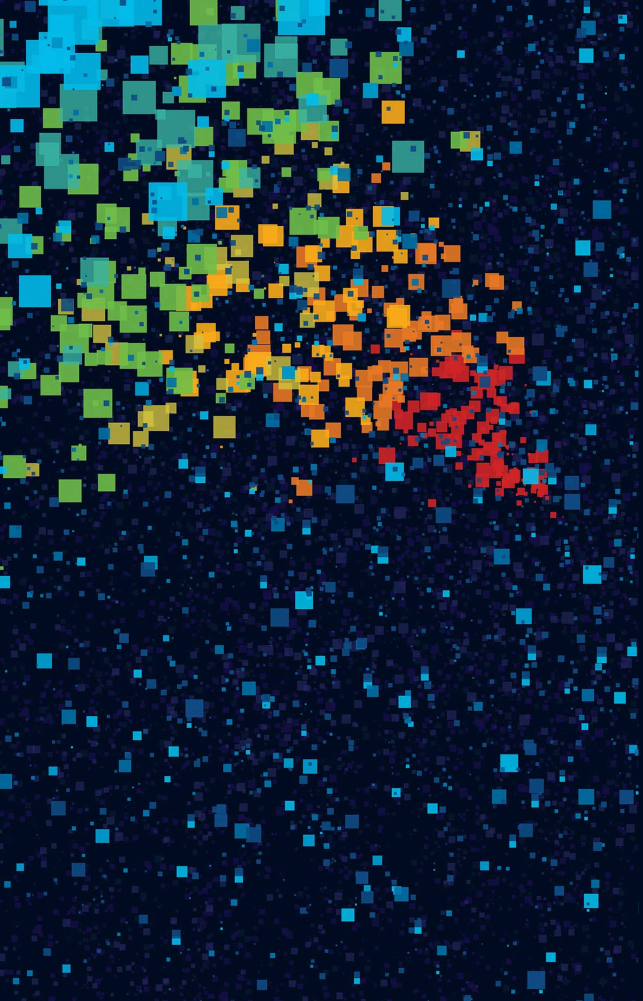
Possibilities

#CiscoLive

How Security Research is Helping Defenders to Stay Ahead of Attackers

Join the race...

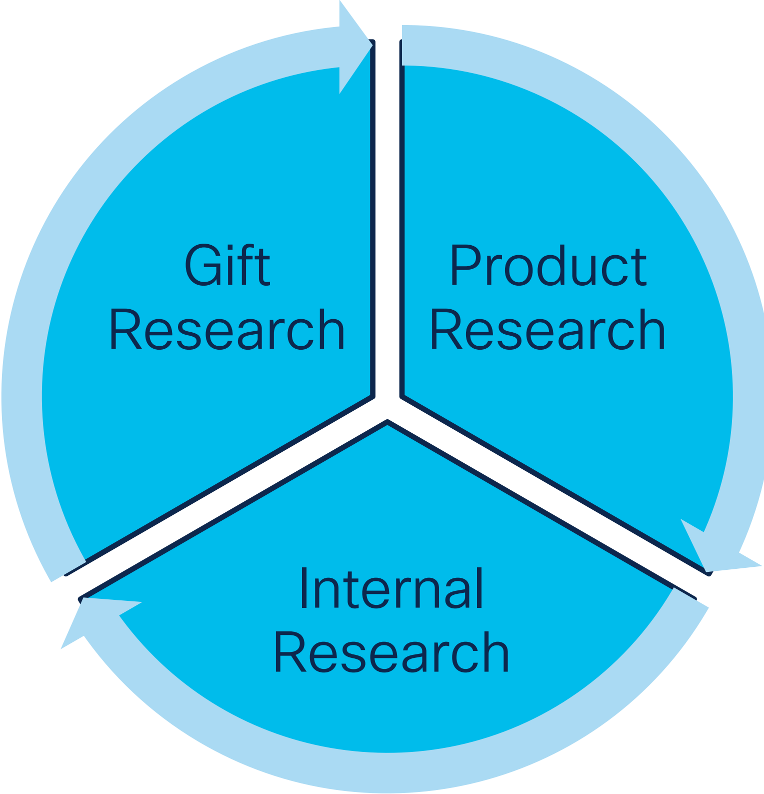
Chris Shenefiel Principal Engineer, Security and Trust
@CShenefiel
DGTL-BRKSEC-1012



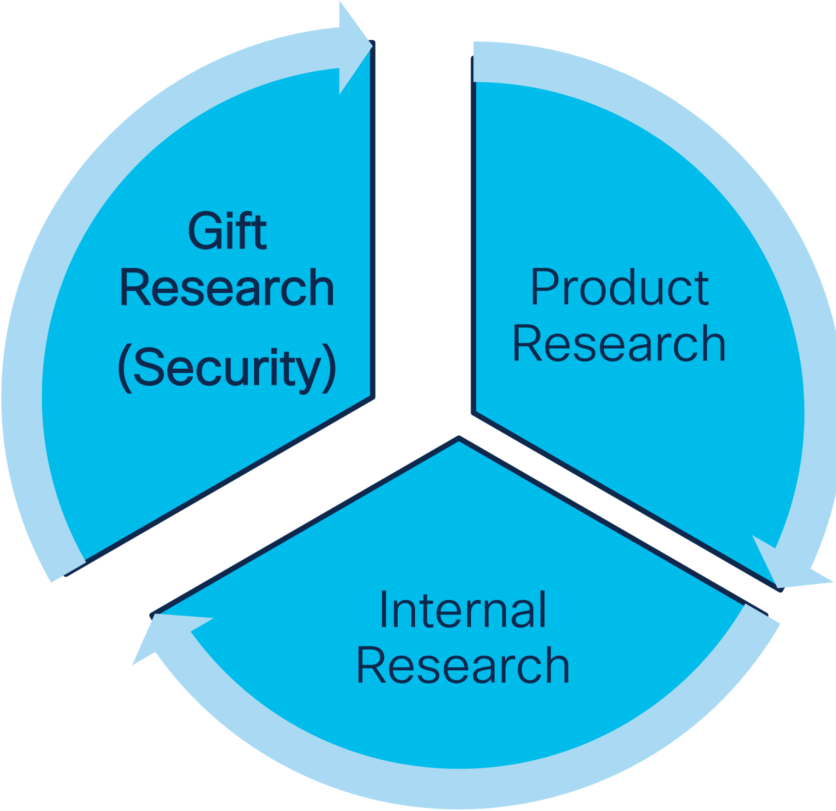
Agenda

- Introduction
- Cisco research
- Security research model
- Security research industry impact
- Future research plans
- Attendee recommendation and advice

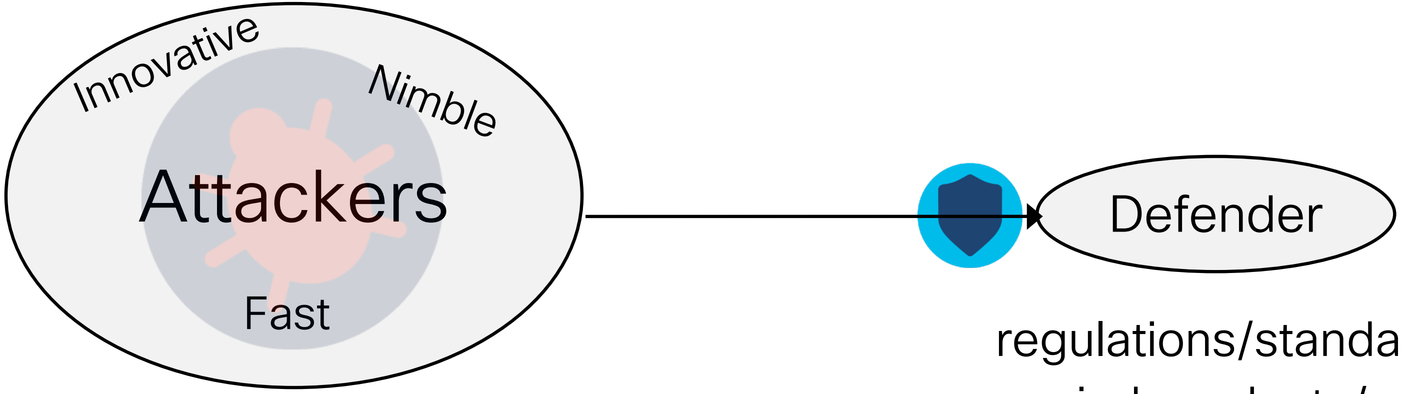
Cisco Research Initiatives



Cisco Research Initiatives



Cybersecurity challenge



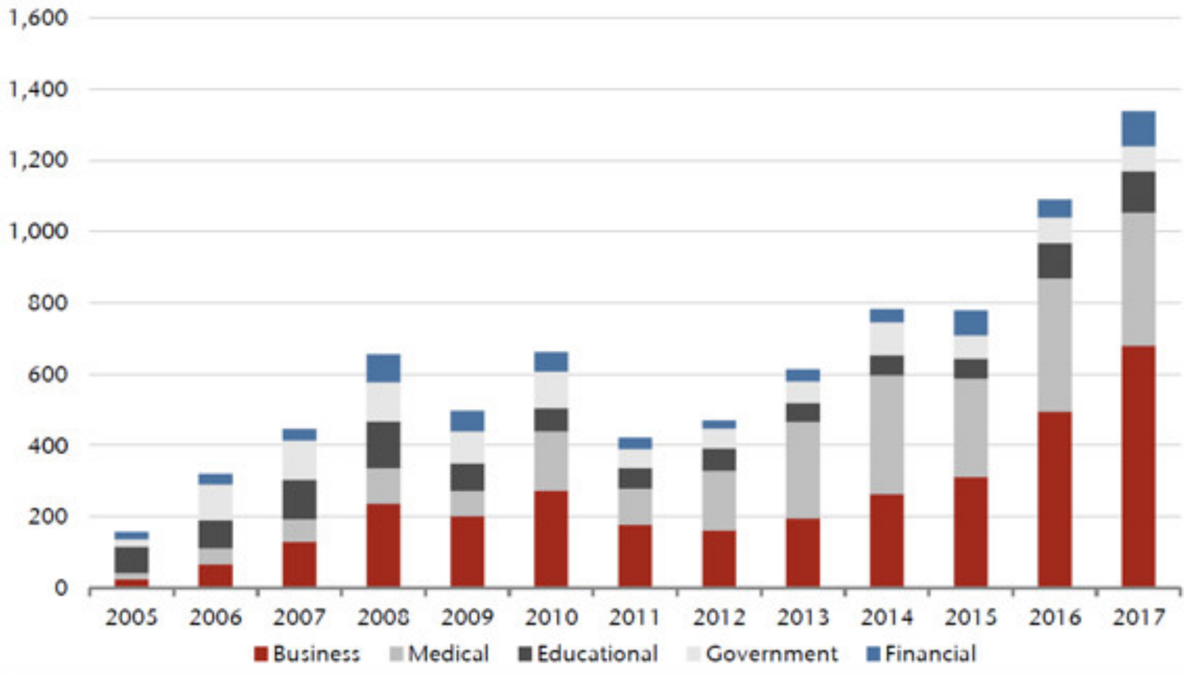
communities
tools
economics

regulations/standards
myriad products/services
limited IT budget

Attacker

Success rate is rising

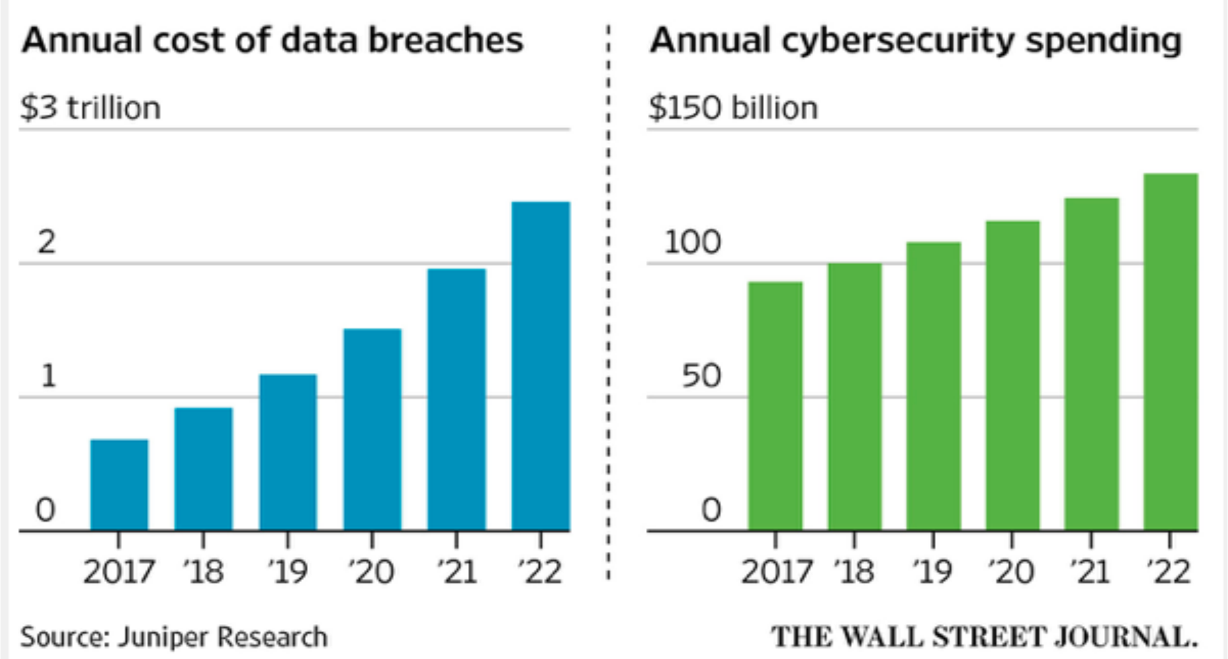
Chart 9: Increasing number of data breaches (by entity)



Source: Jefferies, Identity Theft Resource Centre

Defender

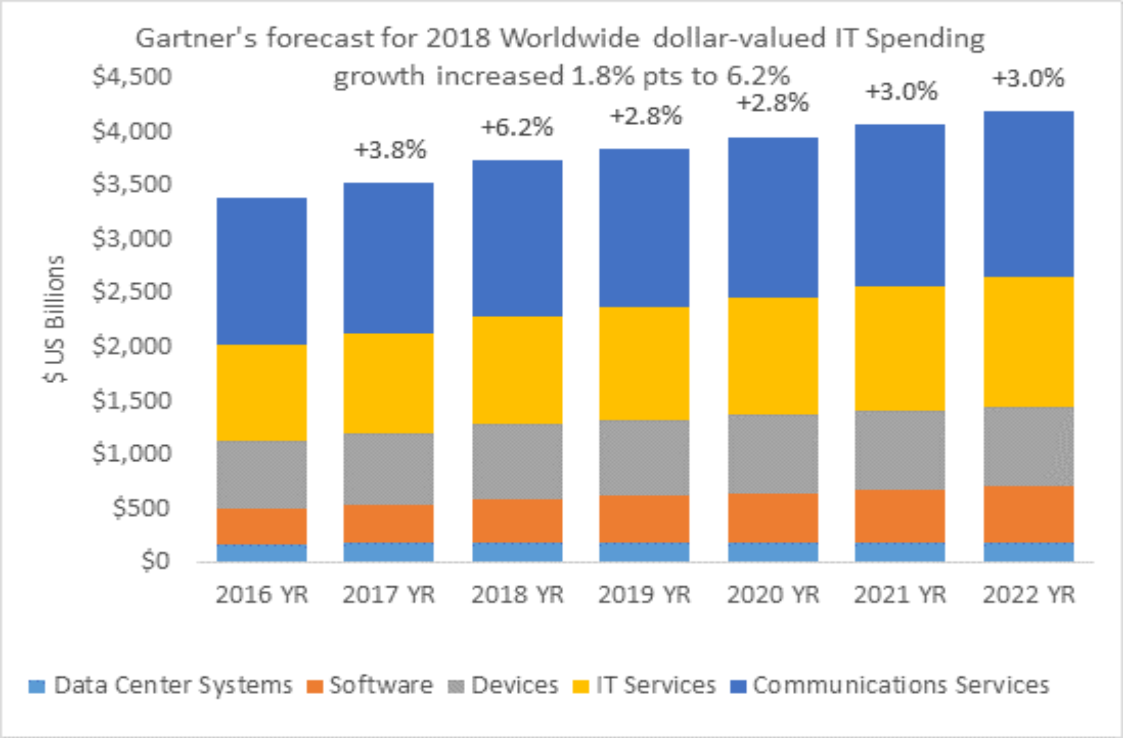
Spending on Cybersecurity defense and breach costs are on the rise



Source: Juniper Research

THE WALL STREET JOURNAL.

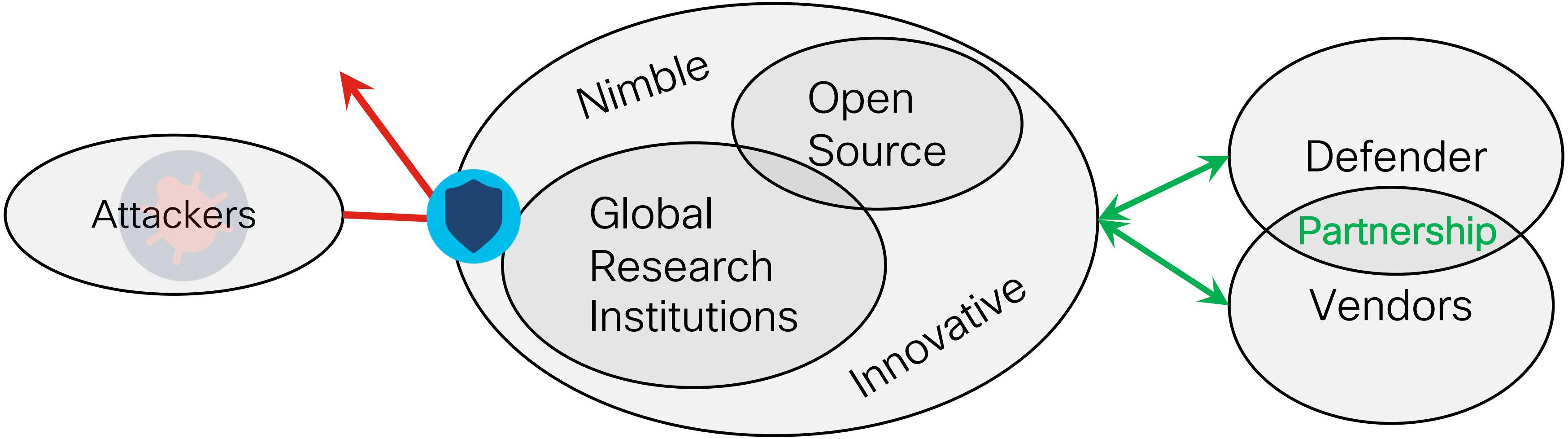
What if each of us granted .01% of IT budget for cybersecurity research?



We could inject $40B into cybersecurity research

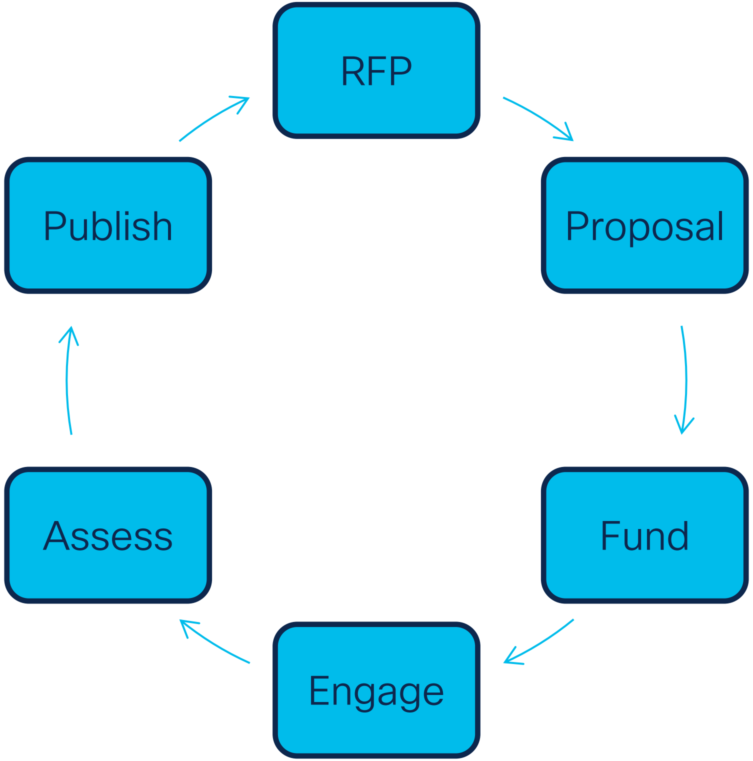
With $40B for research, we could...

Shift the balance



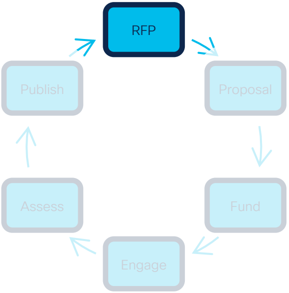
Communities
Tools
Economics

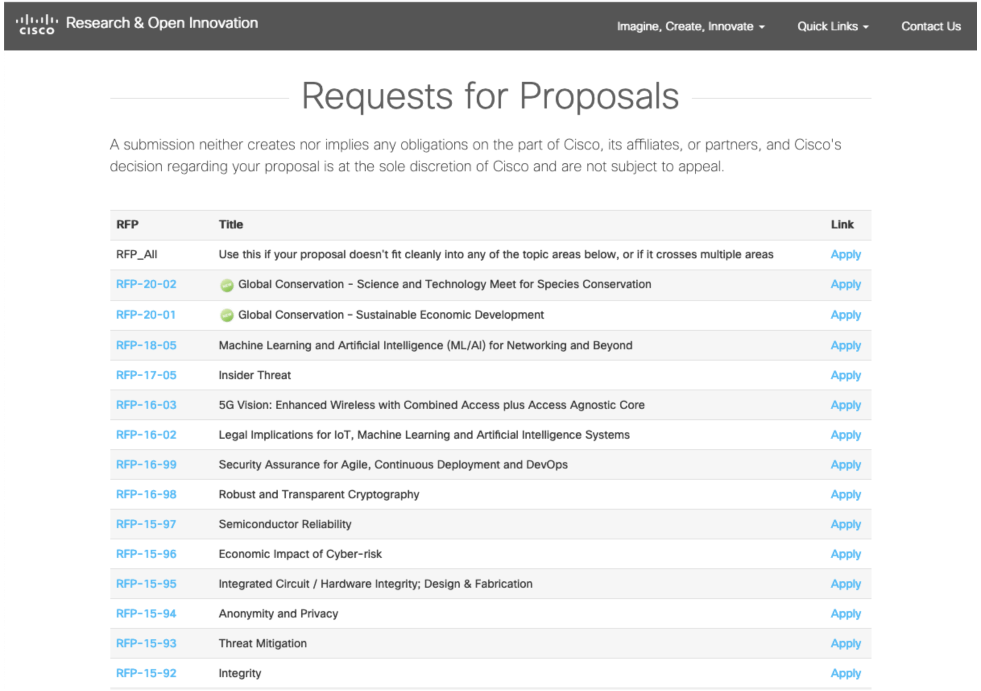
Cybersecurity research at Cisco



RFPs for what we care about

https://research.cisco.com





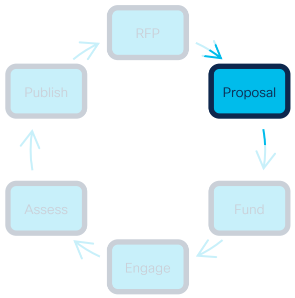
Requests for Proposals

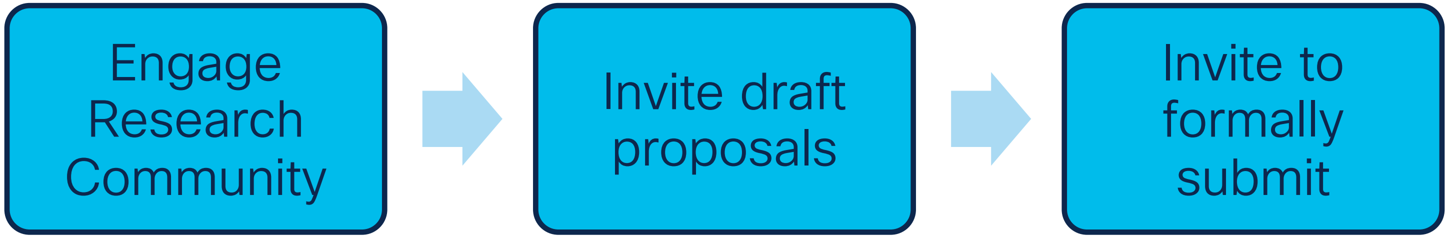
A submission neither creates nor implies any obligations on the part of Cisco, its affiliates, or partners, and Cisco's decision regarding your proposal is at the sole discretion of Cisco and are not subject to appeal.

RFP	Title	Link
RFP_All	Use this if your proposal doesn't fit cleanly into any of the topic areas below, or if it crosses multiple areas	Apply
RFP-20-02	Global Conservation - Science and Technology Meet for Species Conservation	Apply
RFP-20-01	Global Conservation - Sustainable Economic Development	Apply
RFP-18-05	Machine Learning and Artificial Intelligence (ML/AI) for Networking and Beyond	Apply
RFP-17-05	Insider Threat	Apply
RFP-16-03	5G Vision: Enhanced Wireless with Combined Access plus Access Agnostic Core	Apply
RFP-16-02	Legal Implications for IoT, Machine Learning and Artificial Intelligence Systems	Apply
RFP-16-99	Security Assurance for Agile, Continuous Deployment and DevOps	Apply
RFP-16-98	Robust and Transparent Cryptography	Apply
RFP-15-97	Semiconductor Reliability	Apply
RFP-15-96	Economic Impact of Cyber-risk	Apply
RFP-15-95	Integrated Circuit / Hardware Integrity; Design & Fabrication	Apply
RFP-15-94	Anonymity and Privacy	Apply
RFP-15-93	Threat Mitigation	Apply
RFP-15-92	Integrity	Apply

Proposal

Collaborate on research ideas





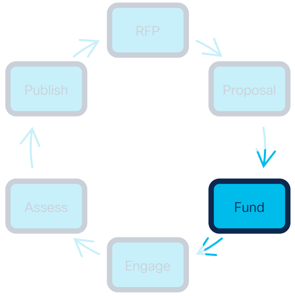
Engage Research Community

Invite draft proposals

Invite to formally submit

Fund

Enable research


RFP

Proposal

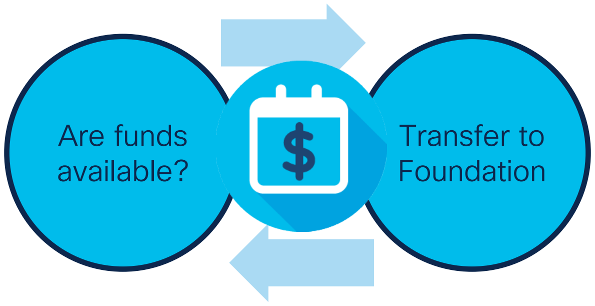
Fund

Engage

Assess

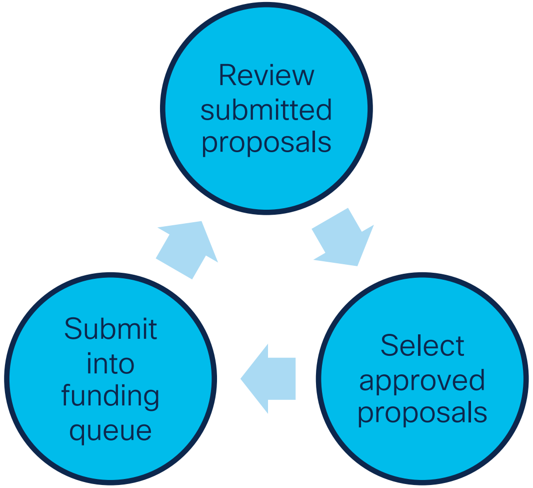
Publish

Research Fund (quarterly)


Are funds available?

Transfer to Foundation

Proposal Review & Award (biweekly)

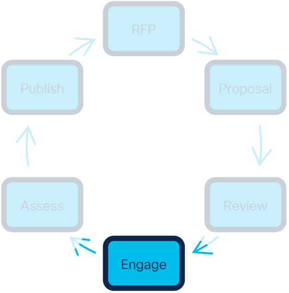

Review submitted proposals

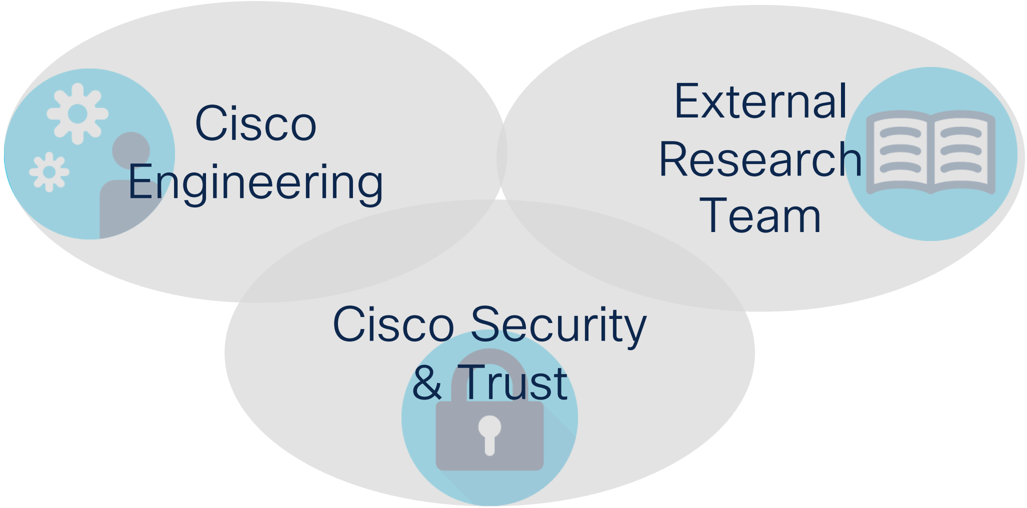
Select approved proposals

Submit into funding queue

Engage

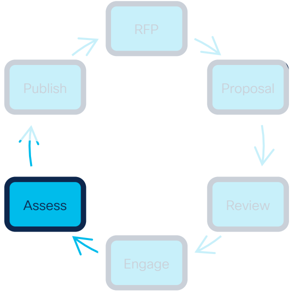
Continuously engage research team throughout project

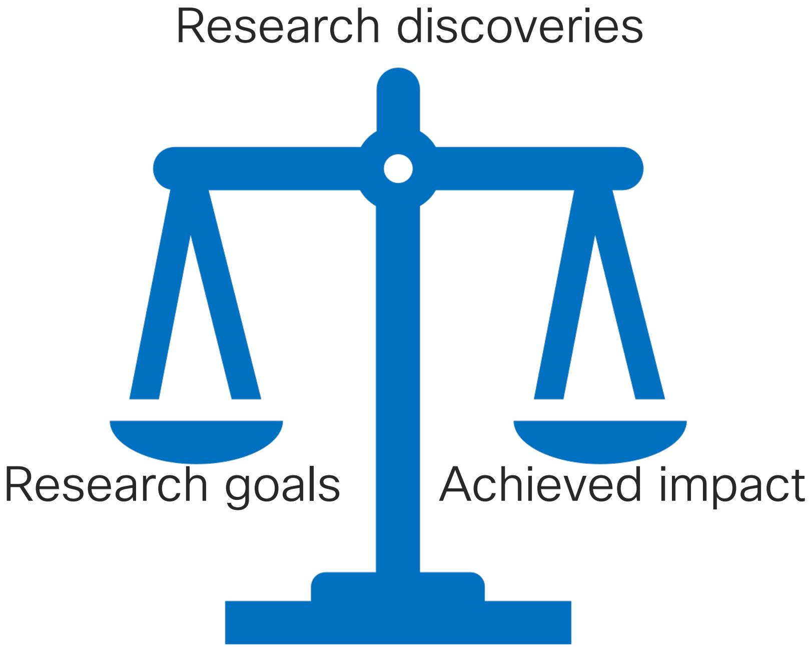




Assess

Fail fast forward





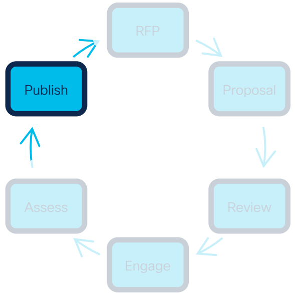
Research discoveries

Research goals

Achieved impact

Publish

Share results and tools



Open Source Tools

Education

Publications

Conferences

Engagement Opportunities

Ways Cisco has engaged with research community

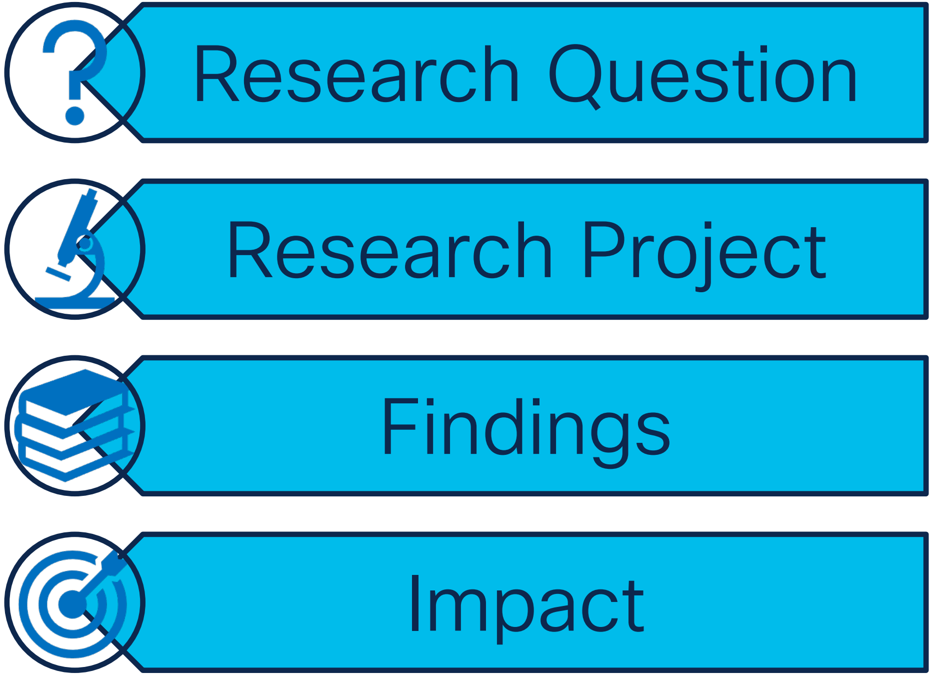
Consortia	NSF Industry University Cooperative Research Centers (http://iucrc.org) INRIA
Research Institutions	Universities Research Foundations (e.g., Fraunhofer)
Grant Model	Gift research grants and silent on IP rights Directed grants; payment on progress and IP rights negotiated up front
Conferences	NDSS, HOST, etc.
Forums	Future Privacy Forum
Open Source	OWASP OpenSSL

How can you engage in research?

- What are your vulnerabilities?
- What are attackers doing to you regularly?
- What is your industry?
- Do you have data that the research industry needs?

Research Stories

Security Research Impact



Research Question

Research Project

Findings

Impact

Boston University Sharon Goldberg NTP Security

Improve open source security

- NTP protocol security
- Study security of NTP
- Three research papers presenting new attacks and new design proposals
- CVE-2015-7704 and security advisories from Juniper, RedHat, IBM, Cisco

https://www.cs.bu.edu/~goldbe/papers/NTPattack.pdf

George Mason Container Security

Improve open source security

- How to improve security for containers?
- Is it possible to dynamically limit system calls at different runtime phases?
- 1 paper and 1 public tool + NSF grant
- Testing tool in production systems

https://github.com/zeyu-zh/speaker

Georgia Tech

Operating system runtime integrity

- Can a running system be continuously monitored for integrity – instead of just at load time?
- Research of securing conventional, virtual memory-enabled operating systems.
- PhD dissertation and prototype system running Linux on a FPGA
- Changes to system and OS design and testing

https://www.mdpi.com/2410-387X/2/3/20

William and Mary Law School ML/AI/IoT Legal Implications

Educate stakeholders and future workforce

How does advanced technology impact corporate risk and legislation

Study legal implications and legislative gaps

3 Law Review articles, judiciary briefings, corporate briefings, student commentaries

Judiciary briefings, 9 student paper awards, new law school curricula, 2 international conferences

https://scholarlycommons.law.case.edu/caselrev/vol68/iss3/14/

https://www.legaltechcenter.net/a-i/commentary/

Fraunhofer Research DNS Cache Security

Inform the industry

- Is DNS for IPv6 vulnerable to the same cache vulnerability as IPv4
- Research DNS cache behavior for public DNS servers
- 1 paper and 1 public tool
- Public site that tests any DNS server's cache vulnerability

http://dns.xray.sit.fraunhofer.de/

Johns Hopkins University: Crypto Done Right

Improve industry security

How to reduce common errors in cryptographic library implementation?

Best practices for good cryptography implementation.

Offer a site https://cryptodoneright.org to publish and share best practices.

The go-to place for learning how to properly implement cryptography

University of Florida FICS Institute

Hardware security using visual inspection

Can physical tampering be detected through image analysis?

BRAND to develop multi-modal image analysis techniques and component identification

Multiple papers on techniques to enable automated detection of components and assembly anomalies

https://arxiv.org/pdf/2002.04210.pdf

IEEE PAINE Conference, participation in DoD supply chain initiative

http://paine-conference.org/

University of Florida FICS Institute

Microelectronics Design for Security

Can some microelectronics security issues be detected during early design?

Multiple projects developing enhanced models for study of power emanations, design tool vulnerabilities

Multiple papers and tools

https://dl.acm.org/doi/10.1145/3133956.3134040

https://arxiv.org/pdf/1803.04102.pdf

Secure design guidelines, support for TRUST HUB, disclosure of IEEE standard vulnerability, early identification of fault- and injection vulnerabilities, etc.

https://trust-hub.org

University of California, San Diego

Sys: Finding hard to detect bugs in open source code

Is it possible to automatically find hard security bugs where easy-to-find bugs have been found by years of aggressive checking?

Can static checkers identifying possible error sites, and symbolic checkers reason about those sites to find bugs?

Sys found security bugs (49 bugs, 39 confirmed) in Chrome and Firefox web browsers and in complex code that confuses existing tools (e.g., FreeBSD)

Paper accepted for publication at USENIX Security '20. Sys open source availability after USENIX presentation.

Inria, TAMIS Group

Automatic Malware Classification

Is there a way to classify malware samples at line rate suitable for use on a high-speed network device?

Combine learning methods with symbolic execution to build an experimental hybrid classifier

Efficient clustering based on System Call Dependency Graphs (SCDGs)

Results published in "Computers & Security 93 (2020) 101775"; detecting new vulnerabilities

Conclusion

- Tilt the balance in favor of the defenders
- Join Cisco in funding cybersecurity research as a partner or on your own
- Support cybersecurity education, research and open source development
- Share your data with researchers

Thank you

Possibilities

#CiscoLive