Scott E. Coull

http://www.scottcoull.com/

Professional Summary

Proven research leader with **over 15 years of experience** driving groundbreaking innovations at the intersection of cybersecurity and AI. Success in leading global teams to develop cutting-edge ML and AI solutions with direct customer impact. Delivered features for products generating $600M+ in ARR and established thought leadership through pioneering research, publications, and invited talks.

Professional Experience

Google Cloud Security (formerly, Mandiant), Mountain View, CA

Head of Data Science Research **November 2022 to Present**
Director, Data Science Research **April 2021 to October 2022**
Sr. Manager, Data Science **January 2019 to March 2021**
Principal Data Scientist **January 2018 to December 2018**
Senior Staff Data Scientist **January 2017 to December 2017**

- Led an international team of ML researchers addressing cybersecurity challenges, including malware detection, threat intelligence, and security operations.
- Delivered innovations integrated into products achieving over $600M in ARR, including:
  - **Sec-PaLM**: Domain-specialized LLM driving Google Cloud Security features.
  - **SecLM**: Agentic platform for supporting advanced security use cases.
  - **MalwareGuard**: Next-gen antivirus deployed to over 2M customer devices.
  - **IC-Score**: Threat intelligence scoring adopted across Google Cloud Security.
- Initiated sponsored research programs with universities, fostering collaboration and advancing adversarial machine learning research
- Created and taught the Data Science 101 curriculum to 200+ global attendees.
- Mentored and scaled a team of 15+ researchers across geographies, promoting cross-functional collaboration.

RedJack, LLC., Silver Spring, MD

Senior Research Scientist **October 2015 to December 2016**
Research Scientist **June 2010 to September 2015**

- Captured $1.2M in new research funding as PI and contributed to $16M in additional projects.
- Developed cryptographic primitives and traffic generation techniques for censorship circumvention.
- Applied NLP to identify child exploitation indicators on Tor hidden services.
- Defined privacy-sharing guidelines for network data, adopted by DHS and FCC

University of North Carolina, Chapel Hill, NC

Postdoctoral Research Associate **May 2009 to August 2010**

Johns Hopkins University, Baltimore, MD

Research Assistant **January 2008 to May 2009**
Teaching Assistant **August 2005 to December 2007**

Sandia National Laboratories, Livermore, CA

Summer Research Intern **June 2006 to August 2006**

Rensselaer Polytechnic Institute, Troy, NY

Teaching Assistant **January 2004 to May 2005**

FX Technologies, LLC, Troy, NY

Consultant **October 2000 to December 2018**

Travelers Insurance, Hartford, CT

Summer Intern - Information Systems Security **May 2001 to August 2001**
Summer Intern - Mainframe Operations Group **June 2000 to August 2000**

Education

Johns Hopkins University, Baltimore, MD

Ph.D., Computer Science, May 2009

- Thesis: Methods for Evaluating the Privacy of Anonymized Network Data
- Advisor: Professor Fabian Monrose

Rensselaer Polytechnic Institute, Troy, NY

M.S., Computer Science, June 2005

- Thesis: Sequence Alignment for Masquerade Detection
- Advisor: Professor Boleslaw K. Szymanski

B.S., Computer Science, December 2003

- *magna cum laude*
- Minor in Information Technology

Awards & Certifications

Mandiant One Team Award

- Digital Risk Protection, 2022
- MalwardGuard Next-Gen Antivirus, 2020

International Information Systems Security Certification Consortium (ISC^2)

- Certified Information Systems Security Professional (CISSP), 2012-2024

Caspar Bowden Privacy Enhancing Technologies (PET) Award

- Outstanding Research in Privacy Enhancing Technologies, Runner-up, 2014

Computing Research Association

- Computing Innovation Fellowship (Award Rate: 11.4%), 2009-2010

Rensselaer Polytechnic Institute

- Stanley I. Landgraf Prize for Outstanding Academic Achievement, 2004
- Founder's Award of Excellence, 2003
- Upsilon Pi Epsilon Computer Science Honor Society, 2002
  - Chapter Secretary, 2002-2004

19th **Annual Computer Security Application Conference**

- Best Student Paper Award, 2003

Professional Service

Program Committees:

International Conference on Information Systems Security (2009); ISOC Network and Distributed Systems Security Symposium (2010); International Symposium on Stabilization, Safety, and Security of Distributed Systems (2010); ACM Workshop on Information Sharing and Collaborative Security (2014, 2015, 2016); USENIX Workshop on Offensive Technologies (2016, 2017); ACM Conference on Computer and Communications Security (2017); Privacy Enhancing Technologies Symposium (2018 - 2020, 2022 - 2024); ACM Workshop on Artificial Intelligence and Security (2019 - 2024); USENIX Security Symposium (2017,2021, 2025); ESORICS (2021 - 2024); IEEE Deep Learning & Security (2022 - 2024); Security Architectures for Generative-AI Systems (2024), Secure and Trustworthy Machine Learning (2024)

Dissertation Committees:

Maxwell Aliapoulios (NYU), Saidur Rahman (RIT), Giorgio Severi (Northeastern)

Book Chapters

[B2] S. Coull, U. Shankar. *"Solving Domain-Specific Problems Using LLMs."*. In A. Gulli, A. Nawalgaria, G. Mollison (Eds.) Generative AI: A Technical Guide by Google Researchers and Engineers. 2024. pp. 530-566.

[B1] S. Coull. *"Traffic Analysis."* In H. van Tilborg and S. Jajodia (Eds.) Encyclopedia of Cryptography and Security. Springer Publishing. 2011. pp. 1311-1313.

Journal Publications

[J8] E. Rudd, D. Krisiloff, S. Coull, D. Olszewski, E. Raff, and J. Holt. *“Efficient Malware Analysis Using Metric Embeddings.”* ACM Digital Threats: Research and Practice (DTRAP) 5.1 (2024): 1-20.

[J7] L. Demetrio, S. Coull, B. Bigio, G. Lagorio, A. Armando, and F. Roli. *“Adversarial EXEmples: A Survey and Experimental Evaluation of Practical Attacks on Machine Learning for Windows Malware Detection.”* ACM Transactions on Privacy and Security (TOPS), 24(4), September 2021.

[J6] S. Coull and K. Dyer. *“Traffic Analysis of Encrypted Messaging Services: Apple iMessage and Beyond.”* ACM SIGCOMM Computer Communications Review, 44(4), October 2014.

[J5] S. Coull, A. White, T. F. Yen, F. Monrose, and M. Reiter. *“Understanding Domain Registration Abuses.”* Computers & Security, 31(7), October 2012. pp. 806-815. (Invited Paper)

[J4] S. Coull, M. Green, and S. Hohenberger. *“Access Controls for Oblivious and Anonymous Systems.”* ACM Transactions on Information and Systems Security, 14(1), May 2011. pp. 1-28.

[J3] C. Wright, L. Ballard, S. Coull, F. Monrose, and G. Masson. *“Uncovering Spoken Phrases in Encrypted Voice over IP Conversations.”* ACM Transactions on Information and Systems Security, 13(4), December 2010. pp. 1-30.

[J2] S. Coull and B. Szymanski. *“On the Development of an Internetwork-Centric Defense for Scanning Worms.”* Computers & Security, 28(7), October 2009. pp. 637-647.

[J1] S. Coull, and B. Szymanski. *“Sequence Alignment for Masquerade Detection.”* Computational Statistics and Data Analysis, 52(8), April 2008. pp. 4116-4131.

Conference Publications

[C20] S. Rahman, S. Coull, M. Wright. *“MADAR: Continual Learning for Malware Analysis with Diversity-Aware Replay.”* In Submission.

[C19] S. Rahman, S. Coull, M. Wright. *“On the Limitations of Continual Learning for Malware Classification.”* In Proceedings of the 1st Conference on Lifelong Learning Agents, August 2022.

[C18] G. Severi, J. Meyer, S. Coull, and A. Oprea. *“Explanation-Guided Backdoor Poisoning Attacks Against Malware Classifiers.”* In Proceedings of the 30th USENIX Security Symposium, August 2021. (Acceptance rate: 18.7%)

[C17] K. Dyer, S. Coull, and T. Shrimpton. *“Marionette: A Programmable Network-Traffic Obfuscation System.”* In Proceedings of the 24th USENIX Security Symposium August, 2015. (Acceptance rate: 15.7%)

[C16] S. Coull and E. Kenneally. *“Toward a Comprehensive Disclosure Control Framework for Shared Data.”* In Proceedings of the IEEE International Conference on Technologies for Homeland Security, November 2013.

[C15] K. Dyer, S. Coull, T. Ristenpart, and T. Shrimpton. *“Protocol Misidentification Made Easy with Format-Transforming Encryption.”* In Proceedings of the 20th ACM Conference on Computer and Communications Security, November 2013. (Acceptance rate: 19.8%, 2014 PET Award Runner-up)

[C14] T. Taylor, S. Coull, F. Monrose, and J. McHugh. *"Toward Efficient Querying of Compressed Network Payloads."* In Proceedings of the USENIX Annual Technical Conference June, 2012. (Acceptance rate: 14.1%)

[C13] K. Dyer, S. Coull, T. Ristenpart, and T. Shrimpton. *"Peek-a-boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail."* In Proceedings of the 33^{rd} IEEE Symposium on Security and Privacy, May 2012. (Acceptance rate: 13%)

[C12] L. Wei, S. Coull, and M. Reiter. *"Bounded Vector Signatures and their Applications."* In Proceedings of the 6^{th} ACM Symposium on Information, Computer and Communications Security (ASIACCS '11), March 2011. pp. 277-285. (Acceptance rate: 16.1%)

[C11] S. Coull, F. Monrose, and M. Bailey. *"On Measuring the Similarity of Network Hosts: Pitfalls, New Metrics, and Empirical Analyses."* In Proceedings of the 18^{th} Annual Network and Distributed Systems Security Symposium, February 2011. (Acceptance rate: 20.1%)

[C10] S. Coull, A. White, T. F. Yen, F. Monrose, and M. Reiter. *"Understanding Domain Registration Abuses."* In Proceedings of the 25^{th} IFIP International Information Security Conference, September 2010. pp. 68-79. (Acceptance rate: 24.5%)

[C9] S. Coull, M. Green, and S. Hohenberger. *"Controlling Access to an Oblivious Database using Stateful Anonymous Credentials."* In Proceedings of the 12^{th} International Conference on Practice and Theory in Public Key Cryptography (PKC), March 2009. pp. 501-520. (Acceptance rate: 25%)

[C8] S. Coull, F. Monrose, M. Reiter, and M. Bailey. *"The Challenges of Effectively Anonymizing Network Data."* In Proceedings of the DHS Cybersecurity Applications and Technology Conference for Homeland Security (CATCH), March 2009. pp. 230-236.

[C7] C. Wright, S. Coull, and F. Monrose. *"Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis."* In Proceedings of the 16^{th} Annual Network and Distributed Systems Security Symposium, February 2009. pp. 237-250. (Acceptance rate: 11.7%)

[C6] C. Wright, L. Ballard, S. Coull, F. Monrose, and G. Masson. *"Spot Me If You Can: Uncovering Spoken Phrases in Encrypted VoIP Conversations."* In Proceedings of the 29^{th} IEEE Symposium on Security and Privacy, May 2008. pp. 35-49. (Acceptance rate: 11.2%)

[C5] S. Coull, C. Wright, A. Keromytis, F. Monrose, and M. Reiter. *"Taming the Devil: Techniques for Evaluating Anonymized Network Data."* In Proceedings of the 15^{th} Annual Network and Distributed Systems Security Symposium, Februrary 2008. pp. 125-135. (Acceptance rate: 17.8%)

[C4] S. Coull, M. Collins, C. Wright, F. Monrose, and M. Reiter. *"On Web Browsing Privacy in Anonymized NetFlows."* In Proceedings of the 16^{th} USENIX Security Symposium, August 2007. pp. 339-352. (Acceptance rate: 12.3%)

[C3] S. Coull, C. Wright, F. Monrose, M. Collins, and M. Reiter. *"Playing Devil's Advocate: Inferring Sensitive Information from Anonymized Network Traces."* In Proceedings of the 14^{th} Annual Network and Distributed Systems Security Symposium, February, 2007. pp. 35-47. (Acceptance rate: 15%)

[C2] S. Coull and B. Szymanski. *"On the Development of an Internetwork-Centric Defense for Scanning Worms."* In Proceedings of the 40^{th} Annual Hawaiian International Conference on System Sciences, Waikoloa, HI, January 2007.

[C1] S. Coull, J. Branch, B. Szymanski and E. Breimer. *"Intrusion Detection: A Bioinformatics Approach."* In Proceedings of the 19th Annual Computer Security Applications Conference, Las Vegas, NV, December 2003. pp. 24-33. (Best Student Paper Award)

Workshop Papers

[W3] S. Coull and C. Gardner. *"Activation Analysis of a Byte-Based Deep Neural Network for Malware Classification."* In Proceedings of the 2nd Deep Learning and Security Workshop (DLS), San Francisco, CA, May 2019.

[W2] O. Suciu, S. Coull, and J. Johns. *"Exploring Adversarial Examples in Malware Detection."* In Proceedings of the In Proceedings of the 2nd Deep Learning and Security Workshop (DLS), San Francisco, CA, May 2019.

[W1] O. Suciu, S. Coull, and J. Johns. *"Exploring Adversarial Examples in Malware Detection."* In Proceedings of the AAAI Fall 2018 Symposium on Adversary-Aware Learning Techniques and Trends in Cybersecurity, Arlington, VA, October 2018.

Manuscripts

[M4] K. Dyer, S. Coull, T. Ristenpart, and T. Shrimpton. *"Protocol Misidentification Made Easy with Format-Transforming Encryption."* Cryptology ePrint Archive 2012/494.

[M3] S. Coull, J. Branch, B. Szymanski, and E. Breimer. *"Sequence Alignment for Masquerade Detection."* Rensselaer Polytechnic Institute Computer Science Technical Report 06-14.

[M2] S. Coull and B. Szymanski. *"A Reputation-based System for the Quarantine of Random Scanning Worms."* Rensselaer Polytechnic Institute Computer Science Technical Report 05-01.

[M1] S. Coull and B. Szymanski. *"Reputation-based Security in Routed Networks."* In Supplemental Proceedings of the International Conference on Dependable Systems and Networks (DSN), Florence, Italy, June 2004.

Invited and Misc. Talks

[I10] S. Coull. *"Paper to Practice: The Importance of Systems Thinking in Machine Learning for Cybersecurity."*. Keynote at AAAI Artificial Intelligence for Cyber Security (AICS) Workshop, Vancouver, Canada, February 2024.

[I9] S. Coull. *"Efficient Malware Analysis Using Metric Embeddings."* Presented at Machine Learning Security (MLSec) Seminar Series, University of Cagliari, Italy, May 2023.

[I8] S. Coull. *"Promises and Challenges of Security in Trustworthy AI."* Presented at the 5th Deep Learning and Security Workshop (DLS), San Francisco, CA, May 2022.

[I7] S. Coull. *"Activation Analysis of a Byte-based Deep Neural Network for Malware Classification."* Presented at the Conference on Applied Machine Learning for Information Security (CAMLIS), Washington, DC, October 12, 2018.

[I6] S. Coull. *"Privacy vs. Security."* Presented at the NIST Cloud Computing Forum, Gaithersburg, MD. July 8, 2015.

[I5] S. Coull. *"How (Not) to Apply Differential Privacy to Anonymity Networks."* Presented at the DIMACS Working Group on Measuring Anonymity. Rutgers University, New Brunswick, NJ. May 30, 2013.

[I4] S. Coull and E. Kenneally. *"A Qualitative Risk Assessment Framework for Sharing Computer Network Data."* Presented at the 40th Research Conference on Communication, Information, and Internet Policy (TPRC). Arlington, VA. September 23, 2012.

[I3] S. Coull. *"Information Leakage in Encrypted Network Traffic: Attacks and Countermeasures."* Presented at the University of Maryland Computer Science Colloquium. College Park, MD. September 20, 2011.

[I2] S. Coull. *"Network Data Anonymization."* Presented at Pennsylvania State University Computer Science and Engineering Colloquium. State College, PA. March 25, 2010.

[I1] S. Coull. *"Toward Privacy Definitions for Anonymized Network Data."* Presented at the 23rd Annual IEEE Computer Communications Workshop. Lenox, MA. October 18-21, 2009.

Posters

[Po3] S. Rahman, S. Coull, M. Wright. *"On the Limitations of Continual Learning for Malware Classification."* Presented at the 44th IEEE Symposium on Security and Privacy, May 2023.

[Po2] O. Suciu, S. Coull, and J. Johns. *"Exploring Adversarial Examples in Malware Detection."* Presented at the 40th IEEE Symposium on Security and Privacy, May 2019.

[Po1] S. Coull, F. Monrose, and M. Reiter. *"Network Data Privacy."* Presented at IPAM Workshop on Statistical and Learning-Theoretic Challenges in Data Privacy. Los Angeles, CA. February 22-26, 2010.

Patents

[Pa11] S. Coull, et al. *"Generative Sequence Processing Model for Cybersecurity."* U.S. Patent Application PCT/US24/44202. August 2024.

[Pa10] C. Galbraith, S. Coull, P. Tully, N. Smith. *"System and Methods for Artificial Intelligence-based Cybersecurity Threat Intelligence."* U.S. Patent Application 18/770,954. July 2024.
[Pa9] D. Krisiloff, S. Coull. *"Structure-Aware Neural Networks for Malware Classification."* U.S. Patent Application 18/490,141. August 2023.

[Pa8] S. Coull, J. Johns. *"Machine Learning Based Threat Hunting."* U.S. Patent Application 18/310,874. May 2023.

[Pa7] S. Coull, J. Johns *"Gamification through Threat Hunt Packs and/or Threat Hunting Functions."* U.S. Patent Application US18/309,392. April 2023.

[Pa6] S. Coull, J. Johns. *"Cyber-Threat Score Generation Using Machine Learning and Reflecting Quality of Sources."* U.S. Patent Application 17/855,255. June 2022.

[Pa5] S. Coull, J. Johns. *"Cyber-Threat Analyses Using Machine Learning and Prior Observations."* U.S. Patent Application 17/855,272. June 2022.

[Pa4] D. Krisiloff, S. Coull. *"Churn-Aware Machine Learning for Cybersecurity Threat Detection."* U.S. Patent 11,568,316. Filed April 2020. Issued January 2023.

[Pa3] S. Coull, D. Krisiloff, and G. Severi. *"System and Method for Heterogeneous Transferred Learning for Enhanced Cybersecurity Threat Detection."* U.S. Patent 11,475,128. Filed August 2019. Issued October 2022.

[Pa2] S. Coull and J. Johns. *"System and Method for Adaptive Graphical Depiction and Selective Remediation of Cybersecurity Threats."* U.S. Patent 11,201,890. Filed March 2019. Issued December 2021.

[Pa1] J. Johns, B. Jones, and S. Coull. *"System and Method for Analyzing Binary Code for Malware Classification Using Artificial Neural Network Techniques."* U.S. Patent 11,108,809. Filed October 2017. Issued August 2021.