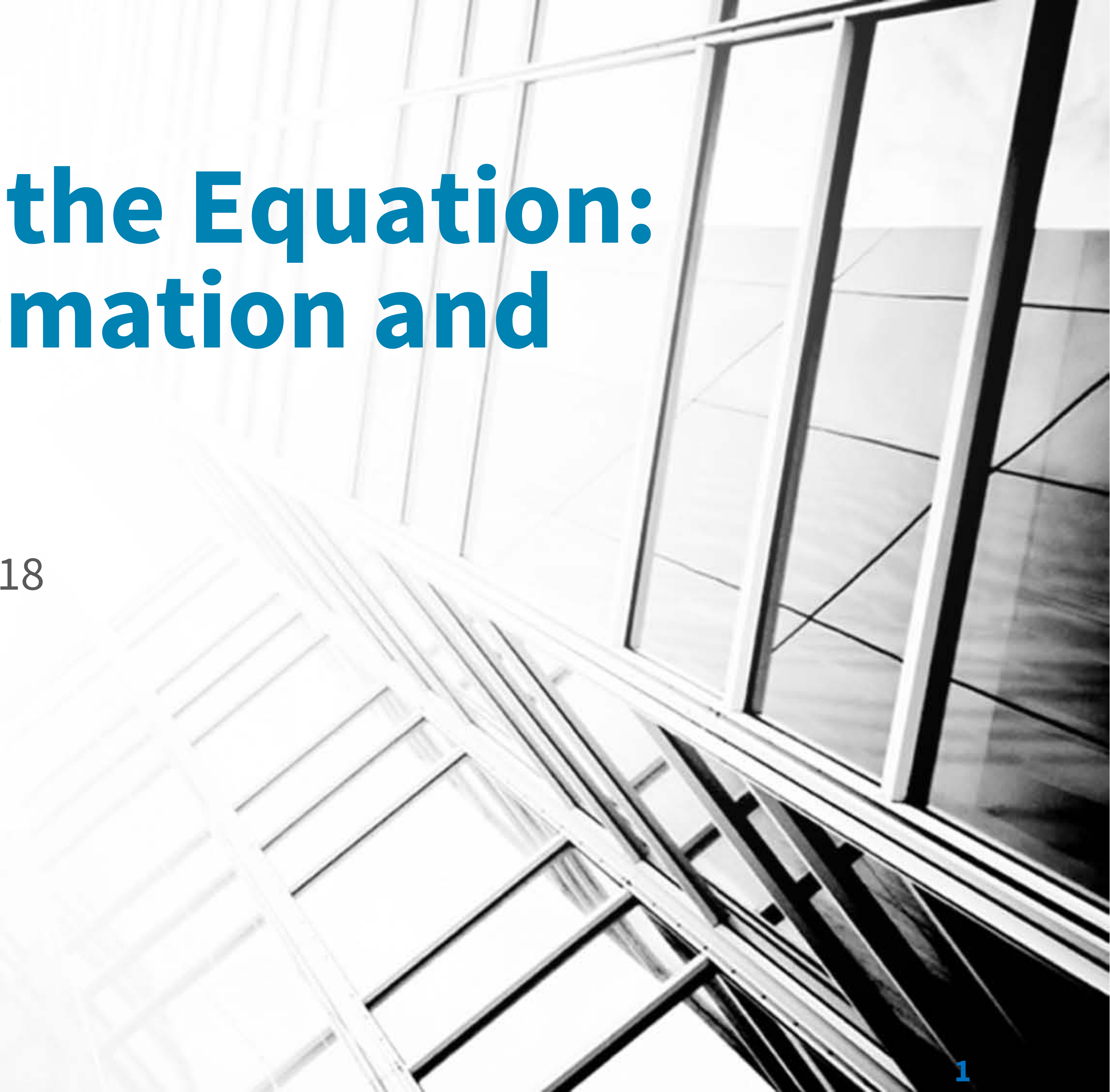
Both Sides of the Equation: Security Automation and Deception

Integrated Cyber - October 2, 2018

Donnie W. Wendt



We are surrounded. Good! Now we can fire in any direction!

Chesty Puller, USMC

Donnie Wendt

Who Is This Guy?

- Security Engineer with MasterCard
- Cybersecurity Professor at Utica College
- Certified Information Systems Security Professional (CISSP)
- MS Cybersecurity with Concentration in Intelligence
- Student at Colorado Technical University
  - Pursuing Doctor of Science – Computer Science - Emphasis in Information Security
  - Area of research – Security Automation and Orchestration
- Interests – Playing guitar, scuba diving, running, and studying history
- LinkedIn - https://www.linkedin.com/in/donnie-wendt-b958a6120/
- Blog – https://www.showmecyber.com

Today’s Topics

Asymmetry and the Attacker’s Advantage

The OODA Loop

Speeding Detection & Response

Slowing the Attacker

Conceptual Framework

Shameless Plug for My Research

Research Question
How have US-based companies in the finance sector implemented security automation and adaptive cyber defenses and what challenges have they faced with the implementation?

Soliciting Participants
Security professionals in the finance industry who are implementing or have implemented security automation.

What is required of participants?
60 – 90 minute interview

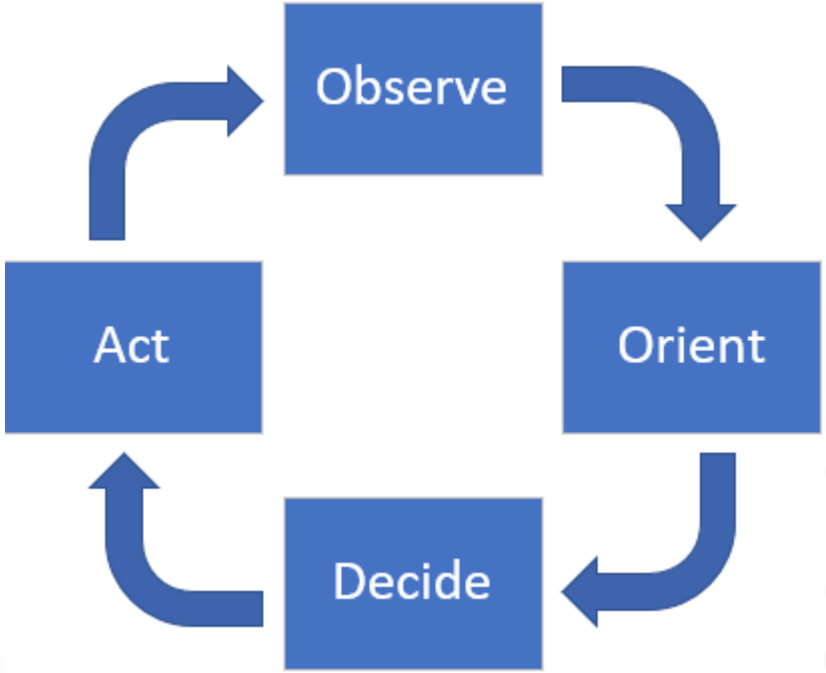
Current State

Advantage Attacker

- Attacker Enjoys an Asymmetric Advantage
    - Exploit one vs. defend all
    - Homogenous platforms and software
    - Well-known static defenses
- Increased Sophistication of Attacks
    - Highly motivated attackers
    - Detection increasingly difficult
- The Need for Speed
    - Human-centered defenses cannot keep pace
    - Defenders must increase speed of detection and response

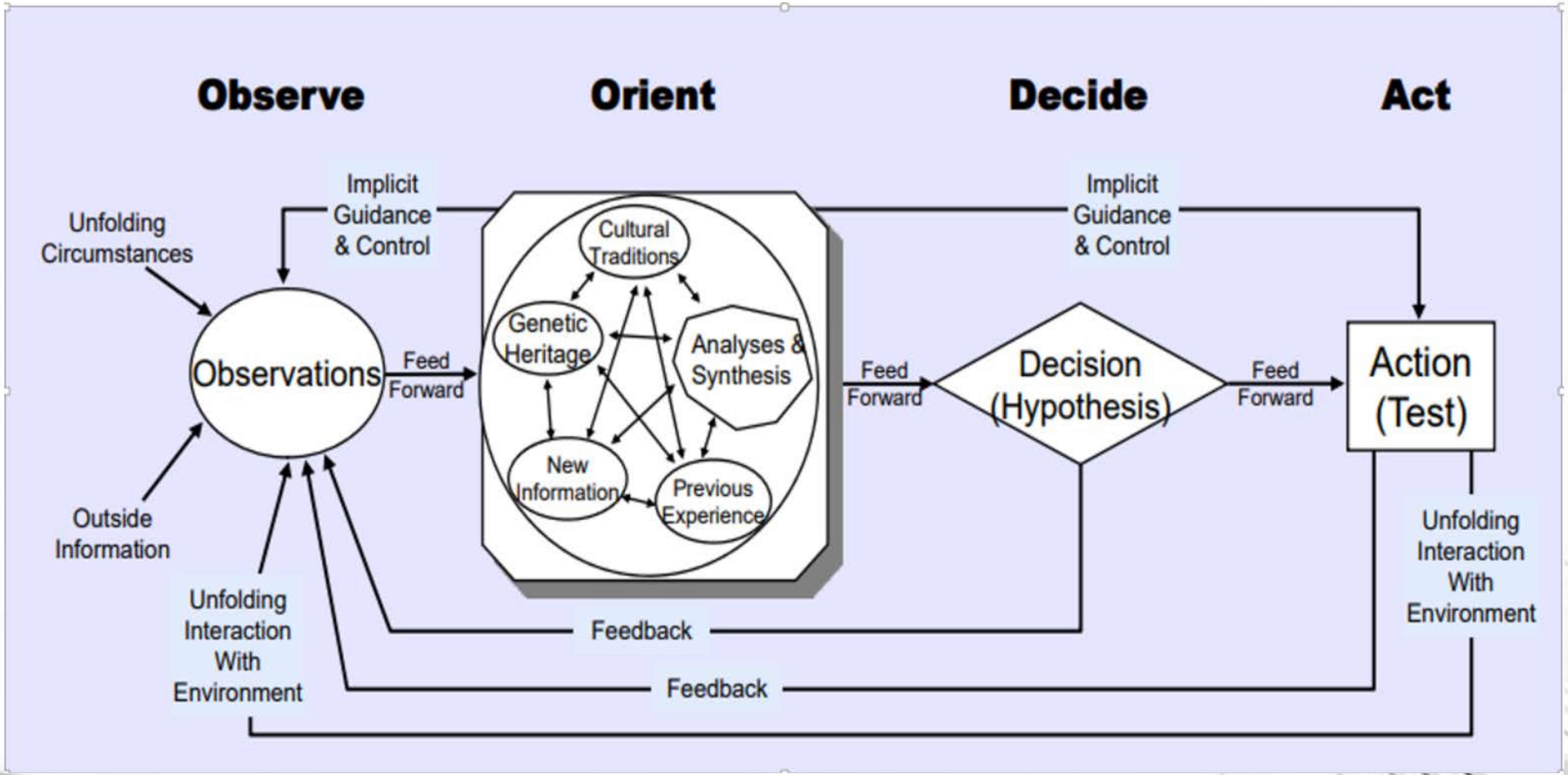
The OODA Loop
Often Referenced, Often Misunderstood

- Developed by Air Force pilot John Boyd
- Refers to gaining superiority in air combat
- Often shown as a four-phase, cyclic process



The OODA Loop

As Drawn by Boyd



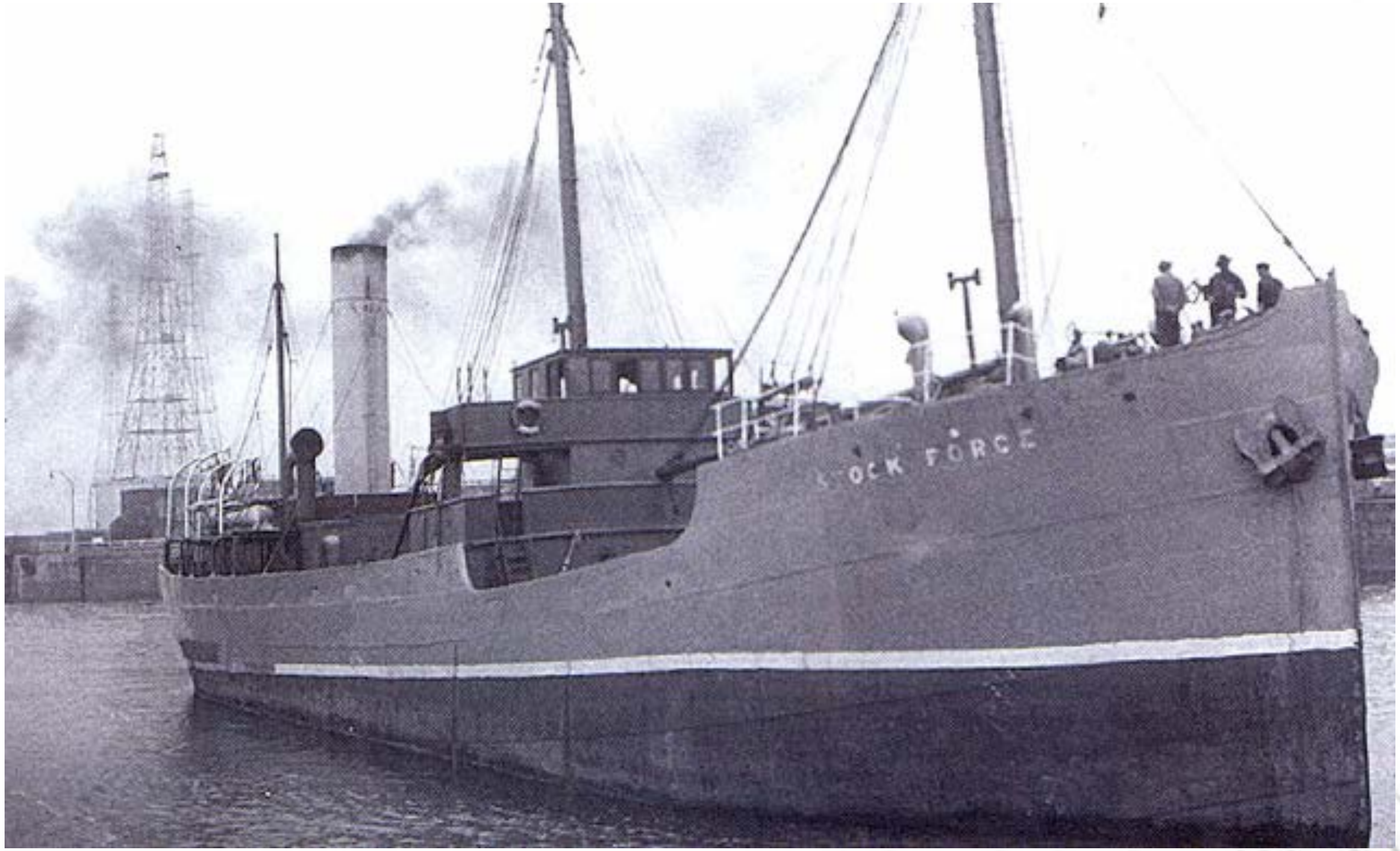
Automation - Speeding the OODA Loop

Continuous Situational Awareness

- Situational awareness requires automation
- IACD – Redefining the OODA loop
- Automated enrichment
  - Improves situational awareness
- Human on the loop
  - Discernment and decision making
- Improving intelligence sharing
  - Decreases attacker’s asymmetric advantage (less exploit reuse)
  - Decreases detection and response times
  - Reluctance and concerns

The British Q-Boats

Using Deception for Defense



Working Inside the Opponent’s OODA Loop

Disrupting Situational Awareness

- Boyd focused on getting inside the attacker’s loop
- Compromise the opponent’s decision-making ability
  - Deceive humans
  - Manipulate data streams
  - Disrupt the opponent’s orientation
- Consume the opponent’s resources
- Improve your own situational awareness
  - Knowledge of opponent

Disrupting the Opponent
Moving Target Defenses

- Diversify critical components
- Temporal Platform Migration
- Platform Diversity
- Concerns with MTD
  - Can Increase Attack Surface
  - Difficult to measure
- Consider the Threat Model

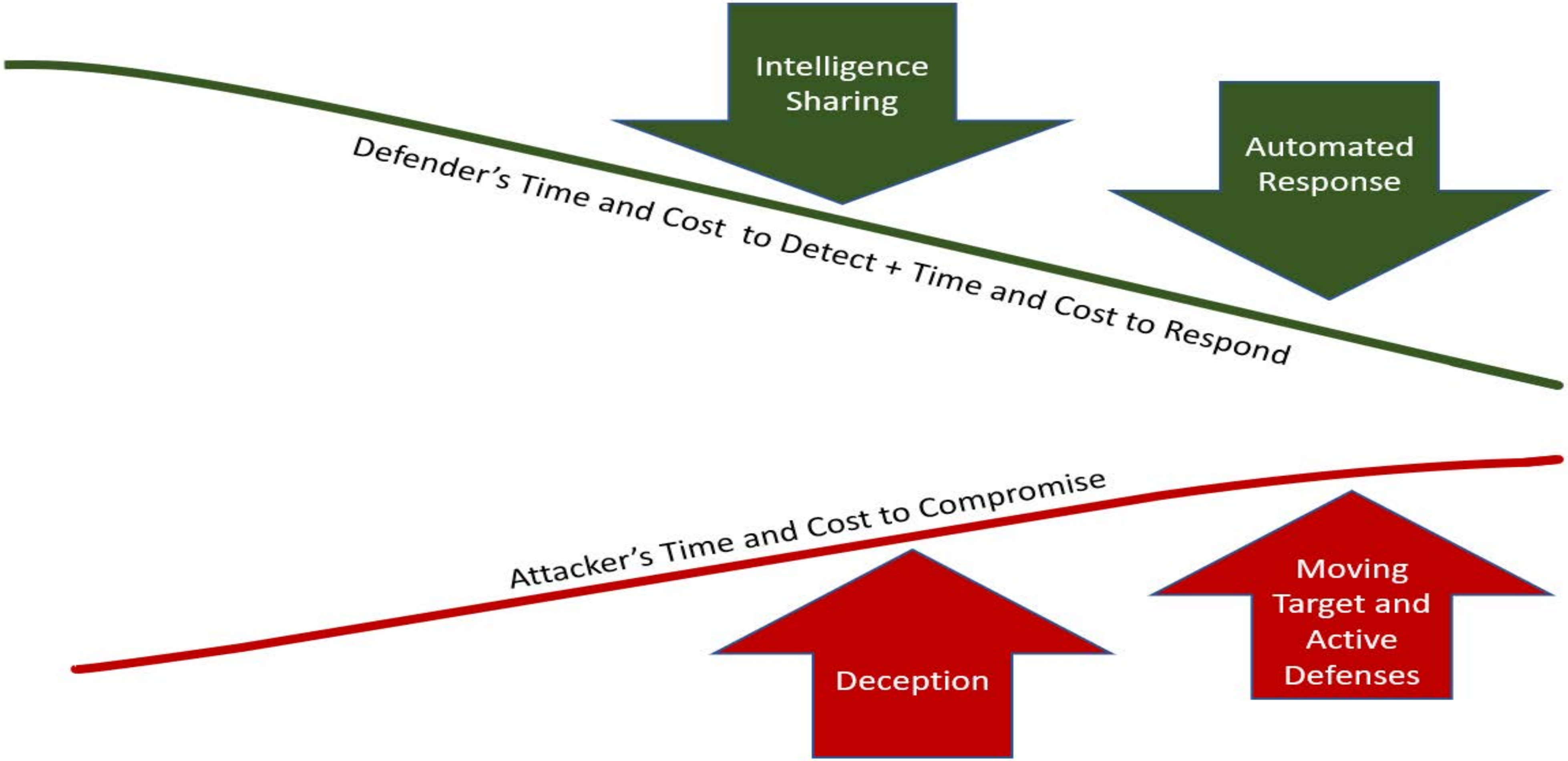
Disrupting the Opponent

Sprinkle in Some Honey

- Applicability of Battlefield Deception
- Deceptive Terrain – Honeypots & Honeynets
- Deploying and Maintaining Honeypots
- Other Deceptions
    - Fake Identities and Beyond
    - Also Used for Insider Threat Detection
- Challenges with Fake Entities

Conceptual Framework

Addressing Both Sides of the Equation



Intelligence Sharing
Automated Response
Defender's Time and Cost to Detect + Time and Cost to Respond
Attacker's Time and Cost to Compromise
Deception
Moving Target and Active Defenses

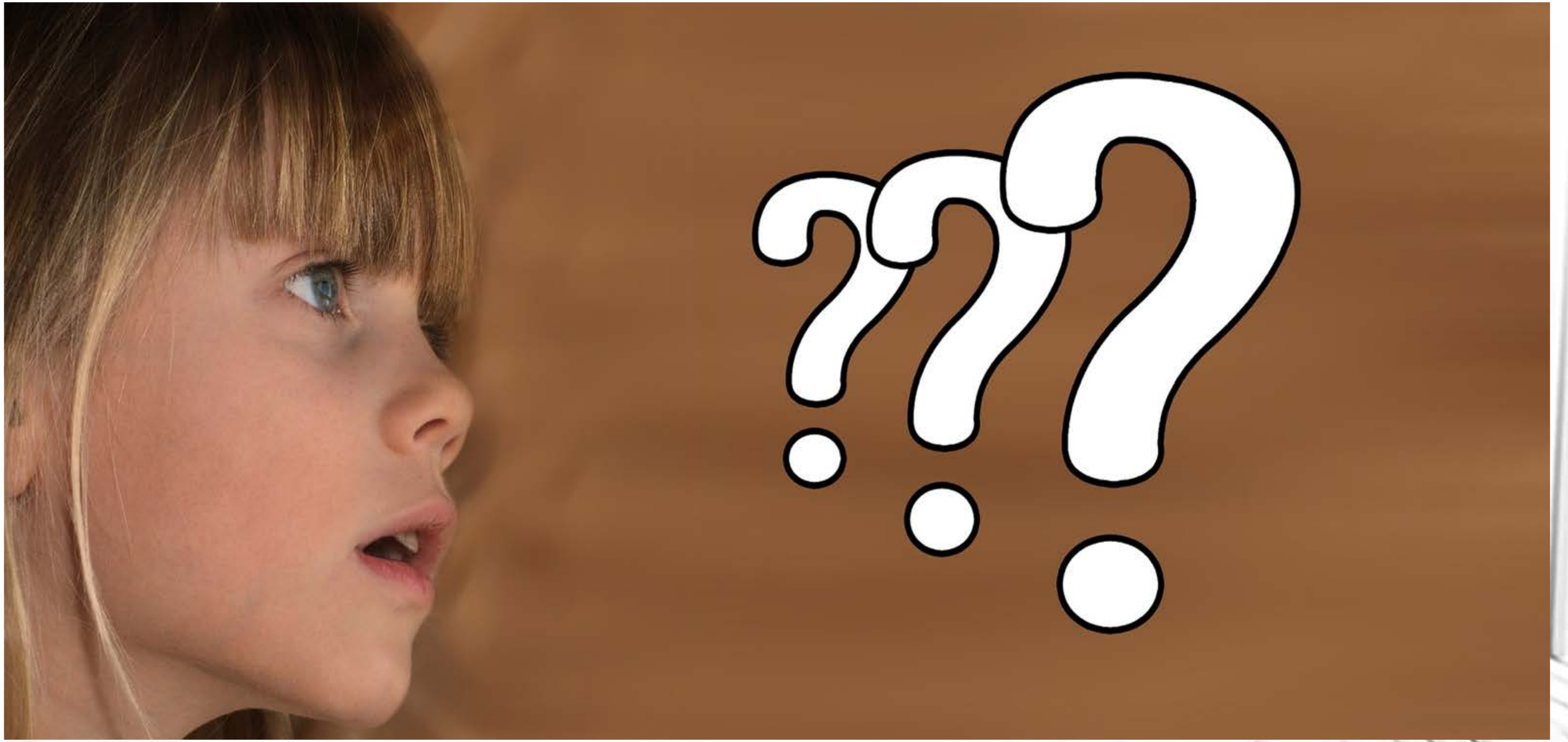
Another Shameless Plug for My Research

Soliciting Participants
Security professionals in the finance industry who are Implementing or have implemented security automation.

What is required of participants?
60 – 90 minute interview

When?
Probably early 2019.

Questions?



References

Standing on the Shoulders of Giants

Al-Ibrahim, O., Mohaisen, A., Kamhoua, C., Kwait, K., & Nijila, L. (2017). Beyond free riding: Quality of indicators for assessing participation in information sharing for threat intelligence. arXiv:1702.00552, 1-12. doi:10.1145/1235

Almeshekah, M. H., & Spafford, E. H. (2016). Cyber Security Deception. In S. Jajodia, V. Subrahmanian, V. Swarup, & C. Wang (Eds.), Cyber Deception (pp. 23-50). Switzerland: Springer. doi:10.1007/978-3-319-32699-3_2

Atighetchi, M., Benyo, B., Eskridge, T. c., & Last, D. (2016). A decision engine for configuration of proactive defenses: Challenges and concepts. Resilience Week (pp. 8-12). Chicago, IL: IEEE. doi:10.1109/RWEEK.2016.7573299

Ben-Asher, N., Alessandro, O., Erbacher, R. F., & Gonzalez, C. (2015). Ontology-based adaptive systems of cyber defense. In K. B. Laskey, I. Emmons, P. C. Costa, & A. Oltramari (Ed.), Semantic Technology for Intelligence, Defense, and Security, (pp. 34-41). Fairfax, VA.

Boyd, J. R. (1986). Patterns of conflict. Retrieved from http://dnipogo.org/john-r-boyd/

Boyd, J. R. (1996). The essence of winning and losing. (C. Spinney, C. Richards, & G. Richards, Eds.) Retrieved from http://dnipogo.org/john-r-boyd/

Brown, S., Gommers, J., & Serrano, O. (2015). From cyber security information sharing to threat management. Workshop on Information Sharing and Collaborative Security (pp. 43-49). Denver, CO: ACM. doi:dx.doi.org/10.1145/2808128.2808133

Byrne, D. J. (2015). Cyber-attack methods, why they work on us, and what to do. AIAA SPACE 2015 Conference and Exposition (pp. 1-10). Pasadena, CA: American Institute of Aeronautics and Astronautics. doi:doi.org/10.2514/6.2015-4576

Carter, K. M., Okhravi, H., & Riordan, J. (2014). Quantitative analysis of active cyber defenses based on temporal platform diversity. OALib Journal. Retrieved from http://arxiv.org/abs/1401.8255v1

Cavelty, M. D. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. Science and Engineering Ethics, 20(3), 701-715. doi:10.1007/s11948-014-9551-y

De Faveri, C., & Moreira, A. (2018). A SPL framework for adaptive deception-based defense. 51st Hawaii International Conference on System Sciences, (pp. 5542-5551). Honolulu, HI. doi:10.24251/HICSS.2018.691

de Fuentes, J. M., Gonzalez-Manzano, L., Tapiador, J., & Peris-Lopez, P. (2017). PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing. Computers & Security, 69, 127-141. doi:10.1016/j.cose.2016.12.011

References

Standing on the Shoulders of Giants

Dewar, R. S. (2017). Active cyber defense: Cyber defense trend analysis. Zurich, Switzerland: ETH Zurich.

Fonash, P. (2012). Identifying cyber ecosystem security capabilities. CrossTalk(September/October), 15-22. Retrieved from https://secwww.jhuapl.edu/IACD/Resources/Reference_Materials/Resilient_Cyber_Ecosystem_Capabilities.pdf

Fonash, P., & Schneck, P. (2015, January). Cybersecurity: From months to milliseconds. Computer, 42-50. doi:10.1109/MC.2015.11

Fraunholz, D., Krohmer, D., Pohl, F., & Schotten, H. D. (2018). On the detection and handling of security incidents and perimeter breaches: A modular and flexible honeytoken based framework. IFIP International Conference on New Technologies, Mobility and Security. Paris, France: IEEE. doi:10.1109/NTMS.2018.8328709

Hong, J. B., & Kim, D. S. (2015). Assessing the effectiveness of moving target defenses using security models. IEEE Transactions on Dependable and Secure Computing, 13(2), 163-177. doi:10.1109/TDSC.2015.2443790

Jhwar, R., Mauw, S., & Zakiuddin, I. (2016). Automating cyber defence responses using attack-defence trees and game theory. The 15th European Conference of Cyber Warfare and Security (pp. 163-172). Munich, Germany: Academic Conferences and Publishing International.

Johns Hopkins Applied Physics Laboratory. (2016). Integrated Adaptive Cyber Defense (IACD) Baseline Reference Architecture. Laurel, MD: Johns Hopkins Applied Physics Laboratory. Retrieved from https://secwww.jhuapl.edu/IACD/Resources/Architecture/IACD Baseline Reference Architecture - Final 0PR.pdf

Johns Hopkins Applied Physics Laboratory. (2017). Integrated Adaptive Cyber Defense (IACD) Orchestration Thin Specification. Laurel, MD: Johns Hopkins Applied Physics Laboratory. Retrieved from https://secwww.jhuapl.edu/IACD/Resources/Specifications/IACD_Orchestration_Thin_Specification.pdf

Kampanakis, P. (2014). Security automation and threat information-sharing options. IEEE Security & Privacy(September/October), 42-51. Retrieved from www.computer.org/security

Lange, M., Kott, A., Ben-Asher, N., Mees, W., Baykal, N., Vidu, C.-M., . . . Madahar, B. K. (2017). Recommendations for model-driven paradigms for integrated approaches to cyber defense. Adelphi, MD: US Army Research Laboratory. Retrieved from https://www.arl.army.mil/www/default.cfm?technical_report=7865

Lenders, V., Tanner, A., & Blarer, A. (2015). Gaining an edge in cyberspace with advanced situational awareness. IEEE Security & Privacy, 13(2), 65-74. doi:10.1109/MSP.2015.30

Machas, A. (2017). Active defense through deceptive IPS. Egham, UK: Royal Holloway University of London.

References

Standing on the Shoulders of Giants

Mermoud, A., Keupp, M. M., Huguenin, K., Palmie, M., & David, D. P. (2018). Incentives for human agents to share security information: A model and empirical test. Workshop on the Economics of Information Security, (pp. 1-22). Innsbruck, Austria. Retrieved from https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS_2018_paper_7.pdf

Mihai-Gabriel, I., & Victor-Valeriu, P. (2015). Cyber incident response aided by neural networks and visual analytics. International Conference on Control Systems and Science (pp. 229-233). Bucharest, Romania: IEEE. doi:10.1109/CSCS.2015.41

Okhravi, H., Streilein, W. W., & Bauer, K. S. (2016). Moving target techniques: Leveraging uncertainty for cyber defense. Lincoln Laboratory Journal, 22(1), 100-109. Retrieved from https://pdfs.semanticscholar.org/15ea/51017d7395fd9cddd626704d1fc82fc42e3e.pdf

Olagunju, A. O., & Samu, F. (2016). In search of effective honeypot and honeynet systems for real-time intrusion detection and prevention. Proceedings of the 5th Annual Conference on Research in Information Technology (pp. 41-46). Boston, MA: ACM. doi:10.1145/2978178.2978184

Rauti, S., & Leppanen, V. (2017). A survey on fake entities as a method to detect and monitor malicious activity. Euromicro International Conference on Parallel, Distributed and Network-Based Processing (pp. 386-390). St. Petersburg, Russia: IEEE. doi:10.1109/PDP.2017.34

Raymond, D., Conti, G., Cross, T., & Nowatkowski, M. (2014). Key terrain in cyberspace: Seeking the higher ground. 6th International Conference on Cyber Conflict (pp. 287-300). Tallinn, Estonia: NATO CCD COE Publications. doi:10.1109/CYCON.2014.6916409

Rege, A. (2016). Incorporating the human element in anticipatory and dynamic cyber defense. IEEE International Conference on Cybercrime and Computer Forensics (pp. 1-7). Vancouver, Canada: IEEE. doi:10.1109/ICCCF.2016.7740421

Richards, C. (2011). Boyd's OODA loop (it's not what you think). Proceedings of the Lean Software & Systems Conference 2011 (pp. 127-136). Sequim, WA: Blue Hole Press.

Saud, Z., & Islam, M. H. (2015). Towards proactive detection of advanced persistent threat (APT) attacks using honeypots. Proceedings of the 8th International Conference on Security of Information and Networks (pp. 154-157). Sochi, Russia: ACM. doi:10.1145/2799979.2800042

Sauerwein, C., Sillaber, C., Mussman, A., & Breu, R. (2017). Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. 13th International Conference on Wirtschaftsinformatik, (pp. 837-851). St. Gallen, Switzerland. Retrieved from http://aisel.aisnet.org/wi2017/track08/paper/3/

Sillaber, C., Mussman, A., Sauerwein, C., & Breu, R. (2017). Data quality challenges and future research directions in threat intelligence sharing practice. ACM Workshop on Information Sharing and Collaborative Security (pp. 65-70). Vienna, Austria: ACM. doi:10.1145/2994539.2994546

References

Standing on the Shoulders of Giants

Soule, N., Simidchieva, B., Yaman, F., Loyall, J., Atighetchi, M., Carvalho, M., . . . Myers, D. F. (2015). Quantifying & Minimizing attack surfaces containing moving target defenses. Resilience Week. Philadelphia, PA: IEEE. doi:10.1109/RWEEK.2015.7287449

Stech, F. J., Heckman, K. E., & Strom, B. E. (2016). Integrating cyber-D&D into adversary modeling for active cyber defense. In S. Jajodia, V. S. Subrahmanian, V. Swarup, & C. Wang (Eds.), Cyber Deception (pp. 1-22). Switzerland: Springer. doi:10.1007/978-3-319-32699-3_1

Tosh, D. K., Molloy, M., Sengupta, S., Kamhoua, C. A., & Kwait, K. A. (2015). Cyber-investment and cyber-information exchange decision modeling. International Conference on High Performance Computing and Communications. New York, NY: IEEE. doi:10.1109/HPCC-CSS-ICESS.2015.264

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & Security, 72, 212-233. doi:10.1016/j.cose.2017.09.001

Virvilis, N., Serrano, O. S., & Vanautgaerden, B. (2014). Changing the game: The art of deceiving sophisticated attackers. 6th International Conference on Cyber Conflict (pp. 87-97). Tallinn, Estonia: NATO CCD COE Publications. doi:10.1109/CYCON.2014.6916397

Willett, K. D. (2015). Integrated adaptive cyberspace defense: Secure orchestration. International Command and Control Research Technology Symposium. Annapolis, MD. Retrieved from https://pdfs.semanticscholar.org/a228/81b8a046e7eab11acf647d530c2a3b03b762.pdf

Winterrose, Carter, K. M., Wagner, N., & Streilien, W. W. (2014). Adaptive attacker strategy development against moving target cyber defenses. ModSim World (pp. 1-11). Hampton, VA: ModSim World.

Zaffarano, K., Taylor, J., & Hamilton, S. (2015). A quantitative framework for moving target defense effectiveness evaluation. MTD’15 (pp. 3-10). Denver, CO: Association for Computing Machinery. doi:10.1145/2808475.2808476

Zager, R., & Zager, J. (2017, October). OODA loops in cyberspace: A new cyber-defense model. Small Wars Journal. Retrieved from https://www.researchgate.net/profile/Robert_Zager/publication/320809843_OODA_Loops_in_Cyberspace_A_New_Cyber-Defense_Model/links/59fb88dd0f7e9b9968ba6bd7/OODA-Loops-in-Cyberspace-A-New-Cyber-Defense-Model.pdf

Zheng, D. E., & Lewis, J. A. (2015). Cyber Threat Information Sharing: Recommendations for Congress and the Administration. Washington, DC: Center for Strategic & International Studies. Retrieved from https://www.csis.org/analysis/cyber-threat-information-sharing

Zhu, M., Hu, Z., & Liu, P. (2014). Reinforcement learning algorithms for adaptive cyber defense against Heartbleed. Moving Target Defense (pp. 51-58). Scottsdale, AZ: ACM. doi:10.1145/2663474.2663481