Jason Wright

Purple Teaming 301– Free Attack Simulation and Alarm/Control Validation

This presentation will be a technical demonstration. It will showcase how to leverage a completely free utility, Atomic Red, to run attack simulations safely in your own organization. Many organizations are puzzled at whether or not they are obtaining the most out oftheir in house SecOps / SOC teams, Managed Security Service Providers, or MDR/EDR suites. Atomic Red Team is an open-source library of tests that security teams can use to simulate adversarial activity in their environments. These tests map to the MITRE framework to validate control operation and verify alarms through detection mechanisms. Creating local accounts, domain accounts, Process Inject/ Hollowing via Powershell and Obtaining Credentials from Password Stores. This presentation will cover why to run this type of simulation, the principles of purple teaming, the technical prerequisites to achieve this in a lab environment (great for students!) or a dev environment, the architecture of the lab in this use case, several Atomic Red simulations via recorded demos and finally how to use this information to improve an organizations detection and response program and get the most out of one's MSSP.

Biography

Jason Wright is an IT and Cybersecurity Professional with over a decade of experience across several industries, such as critical supply chain and financial sectors. Jason primarily serves as a Senior Security Engineer for Convera, a global finance organization, specializing in security operations. Jason also serves as Adjunct Faculty at Chesapeake Community College in the Computer Science and Technology program. Jason possesses several industry certifications, such as the CISSP and Sans GIAC GCIH among others. Jason currently lives in Delmar, Delaware with his wife.