GSAW 2020 Tutorial J:

Moving From Reactive to Pro-Active Cyber Resiliency

Length: Half day

Overview:
The course will define a proactive cyber resiliency approach (Prosilience) to protecting Ground System Architectures using a three phase approach.

New techniques and preemptive threat intelligence are setting the state for machine learning/artificial intelligence convergence which is driving cyber resiliency to a level beyond what is currently performing today.

Phase 1: Define the Baseline

#1: To deliver better, real-time situational awareness that also incorporates more exhaustive scan data, there is a proven approach that merges standard network scans with device configurations, producing exceptionally detailed network diagrams automatically. This approach discovers every device in the infrastructure, not just the devices that are "known." More importantly, the methodology graphically depicts how the devices relate to one another, delivering unfettered situational awareness to instantly prioritize vulnerabilities based on actual risk and their associated impacts. Furthermore, the software automatically and instantly models access flow, visualizes attack paths, clearly identifies the most egregious pivot attack threats, visualizes policy violations, and confirms graphically the security impact of change, resulting in better, faster aggregated cyber situational awareness.

#2: Scanning for vulnerabilities is always important, the challenge is scanning alone will not find the most dangerous unseen vulnerability: The Hidden threat stealthily concealed in the enterprise. It's not just finding known vulnerabilities, it's equally important, if not more important, to find the threat lurking quietly inside the network; that in-and-of-itself is a foremost vulnerability. To find these hidden spies, organizations need to employ an Active Adversary Pursuit methodology in conjunction with an Intelligent Hunt Tool. The methodology and tool is a collection of manned and automatic defensive operations designed to identify, analyze, and eradicate cyber threats inside the network. The approach/tool proactively, preemptively identifies and counters threats that may already reside inside the uncontested conceded space. The Real-time operations identifies signs of planned and active attacks, and very intelligently executes actions to neutralize them.

Phase 2: Automatically Protect the Enterprise

#3: Zero Day vulnerabilities are virtually impossible to stop because they have never been seen before, hence they can't be identified with any vulnerability scan. Exacerbating the Zero Day vulnerability situation are vulnerable applications that have either not been scanned using an application vulnerability scanner (network vulnerability scanning doesn't find application vulnerabilities) or when application changes have been made, application vulnerability scanning wasn't performed. The third vulnerability that constantly rears its ugly head are un-patched systems. These three vulnerability challenges, Zero Day, embedded application vulnerabilities and un-patched systems create cyber volatility.

There now exist a disruptive, proven pro-active approach to literally stop Zero-Day execution, successful attacks on unpatched systems and vulnerable applications. It is a method that kills malware execution at the CPU Memory Level by deploying a small piece of code that monitors and halts attacks before they can execute regardless of malware type. This guardrail code will instantaneously terminate any malware trying to execute on any virtual or free standing server (a Prosilience approach). This guardrail code is NOT signature based, it is based on the behavior of applications mapped to a server's CPU Memory. This technology helps ensure Operational Mission success without interruption

#4: A new highly intelligent, disruptive Machine Learning technique that auto-detects the buildup of cyber-

attack infrastructures during their creation well before an attack commences in now available. The method has a very high accuracy of detecting threat assaults, on average, 51 days in advance of an attack. The benefit is that users will know what is coming well ahead of time and be able to prepare for an attack by pro-actively detecting the attack prior to the event, deceiving the attack, and developing an automated response. Most importantly, using this advance threat prediction Machine Learning tool successfully defeats the well-crafted attack before it even starts.

Phase 2: Automate Response and Remediation

#5: SOAR (Security Orchestration, Automation and Response) combines processes and tools working in concert to automate otherwise disparate security tasks that can be tedious and time-consuming. SOAR not only automates repetitive tasks; it can quickly discern the criticality and legitimacy of an alert and, when desired, initiate automatic remediation. SOAR moves alert determination from minutes to seconds and associated remediation from hours/days to minutes (and sometimes-even seconds). SOAR can automate tasks such as: Synthesizing and responding event data from Security Incident and Event Managers, Intrusion Detection System/Intrusion Prevention System, User & Entity Behavioral Analytic tools such as Bay Dynamics, Advanced Threat Detections Tools, Sandbox technologies, and other tools that report alerts;

- Executing incident investigation using log gathering and analysis;
- Reviewing and analyzing threat intelligence sources;
- Updating tickets, creating reports, and forwarding email alerts;
- Simultaneously logging into multiple systems and enter incident details;
- Understanding context and take corresponding corrective actions;
- Security Operations case management for team overviews, collaborations & information sharing;
- Enrich asset discovery via Configuration Management integration.

SOAR platforms engage the security operations team at the onset by quickly supplementing an incident, assigning owners, and establishing resolution periods that correspond with the severity and sensitivity of an alert/incident. SOAR automatically identifies key attributes of an alert/incident, all endpoints, URLs, machines, hashes, IOC's, files, and all affected assets, delivering a very rich data set instantaneously.

#6: There are over 150 different sources producing over 5,800 relevant reports (classified and unclassified) published every month in 195 unique formats of unstructured reports with 9,500 newly identified indicators to investigate each month. Attempts to manually understand and respond are unsustainable. Now there is an application that automates the discovery and collection of cyber intelligence reports; automates the extraction and correlations of actionable information; orchestrates decision making and automatically identifies effective mitigation while orchestrating the creation, testing, and deployment of sensor signatures. This solution is another building block of Prosilience.

Combining the tools and techniques above will catapult users to the next generation of cyber resilience: Prosilience. The key is to deploy the techniques together so they work harmoniously with each other thereby delivering resilience with consciousness of environment, self-awareness, and the capacity to evolve automatically.

Instructor: Barry Lyons IV, KPMG LLP

Biography:
Mr. Lyons has extensive, wide ranging, leading edge Cyber/ Information Assurance (IA) security expertise and Solutions Architect (SA) systems engineering and software applications experience focusing on the architecture, design, implementation, management and operations of mission critical enterprise systems, airborne solutions, cross domain information sharing solutions, comprehensive identity management solutions (IdM), "Need to Know/Need to Share" On Demand Information Delivery solutions, along with leading Accreditation teams for major systems. Mr. Lyons is known for his innovative approaches to solve

the most demanding situations using commercial products in a very unique way.

Description of Intended Students and Prerequisites:
Basic understanding of cyber principles.

What can Attendees Expect to Learn:

1. Attendees will walk away with actionable knowledge of how to move from a reactionary cyber state to a pro-active cyber position.
2. Attendees will understand how to move the cyber vulnerability paradigm, specifically, understand how to move from knowing what each device does in an enterprise to knowing how the devices relate to one another and why that is so important, also how to move from knowing vulnerabilities to prioritizing vulnerabilities and the actual risk and impact before initiating a change.
3. Attendees will learn the difference between “hunting” and “intelligent hunting” in the concealed uncontested live-memory computer location; how to pro-actively protect un-patched applications; how to obtain threat information up to 51 days before a threat initiates an attack; how to move incident response times from hours to seconds.