SEAS-8414

Analytical Tools for Cyber Analytics

Survey of analytical tools for analyzing cyber security data with particular attention to the use of data analytics procedures in supporting appropriate cyber security policy decisions.

Dr. M

Welcome to SEAS Online at George Washington University

SEAS-8414 class will begin shortly

- **Audio:** To eliminate background noise, please be sure your audio is muted. To speak, please click the hand icon at the bottom of your screen (**Raise Hand**). When instructor calls on you, click microphone icon to unmute. When you've finished speaking, ***be sure to mute yourself again***.
- **Chat:** Please type your questions in Chat.
- **Recordings:** As part of the educational support for students, we provide downloadable recordings of each class session to be used exclusively by registered students in that particular class for their own private use. Releasing these recordings is strictly prohibited.

Agenda

Week-10: Collaborative security analytics tools

We will wrap-up the course with hands-on exposure to the tools in from the following collaborative security category:

- Security Threat Intelligence (STI)
- Threat hunting
- Security Intelligence Graphs (SIG)

Goal of the Lecture

For the last lecture, I would like you to submit either a cybersecurity problem from your work (obfuscating PII and confidential information) or a research problem for your praxis. We will pick three problems and collectively develop security architecture (and map controls) together in the class.

Final Exam

Format

- 50 Questions
    - Multiple choice
    - True-False
    - Multiple Answers

Content

- Content from all 10 classes
- Review lecture recordings
- Lecture slides
- Questions from Lecture-9

Final Exam Topics

- Stateful vs. stateless protocols: HTTP, HTTPS, LDAP, DNS, SSH, SMTP, etc.
- Learn about AWS Security Services: AWS Config, AWS guard duty, AWS security hub, AWS Inspector, AWS Certificate manager, AWS CloudHSM, AWS Macie, AWS EBS.
- Default keys used by different AWS services, AWS managed keys, customer keys, key management,
- Hash function (CRC32, Adler, Murmur) vs. cryptographic hash function (SHA1, MD5, BLAKE)
- Network routed protocols vs. routing protocols.
- Definitions for IP Sniffing, network eavesdropping, spoofing, IAM, Identity broker, Identity provider, SCP, client pool, identity pool, Threat Intelligence, fast-flux domains, phishing domains, disposable domains, C2 domains, cross-site request forgery, server-side request forgery, drive-by malware,

Final Exam Topics

- Definitions for DCA, DPI, DLP, Insider threat detection, Intrusion detection vs. prevention, Web application firewall (WAF), scrapers, scanners, probes, threat modeling, reconnaissance, pen testing, BGP, TCP, UDP, IPv4, SCP, WAF, IDS, IPS, DLP, Terraform, Docker, Scoutsuite, ZAP Proxy, Cloud characteristics, Threat modeling, CSPM, CWPP, CASB, Zero Trust System, False positive, Trust computing base, MiTM, watering hole, eavesdropping, ransomware, Splunk index summary, hot bucket, cold bucket,

- Insider threat motivations, implementation problems, link analysis, different indicators and what can be inferred from them, background indicators, performance review indicators, abductive reasoning, link analysis, log-based indicators

Final Exam Topics

- Different types of data analytics, descriptive, predictive, diagnostics, predictive,
- Purpose and type of Splunk charts - column, area, line, pie, bar
- Research stages, problem statement, thesis, hypothesis, research objectives, literature review, methodology,
- Docker, Namespaces, CGroups
- IP ranges - valid Internet range and private range