Threat Hunting with ELK training

Description:

This hands-on training will walk attendees through leveraging the open source ELK (Elastic) stack to analyze logs to proactively identify malicious activity. The basic tools and techniques taught during this class can be used to investigate isolated security incidents or implemented at scale for continuous monitoring and hunting. Attendees will be provided with access to a preconfigured ELK cluster and extensive sample logs containing diverse malicious events waiting to be discovered on a simulated enterprise network. Attacker artifacts will be mapped to the MITRE ATT&CK Framework and tagged accordingly in the provided logs to help demonstrate the value of log enrichment and a methodological approach to adversary and anomaly detection. The training will conclude with a friendly CTF to give attendees an opportunity to collaborate and compete on teams in order to put their learning into practice.

Course Breakdown - Day 1:

- Introduction to Log Monitoring and Analysis
- Comparative pros and cons of Security Information and Event Management (SIEM) solutions, Splunk, and ELK (Elastic) Stack
- Different types of relevant log sources and logs
- Log shipping, collection, indexing, and searching fundamentals
- Log correlation and enrichment using additional data sources
- How network perimeter and endpoint security logs complement each other
- Introduction to Threat Hunting
- Where threat hunting fits into your security program
- Network security monitoring vs. threat hunting vs. IR/forensics
- MITRE ATT&CK Framework and the cyber attack kill chain
- The role of threat intelligence
- Identifying and hunting for Indicators of Compromise (IOCs) and attacker Tactics, Techniques, and Procedures (TTPs)
- Introduction to the ELK (Elastic) Stack
- Deploying and using the ELK stack
- Elasticsearch (index and search backend)
- Logstash and Beats (log shaping and shipping)
- Kibana (search and visualization/dashboard frontend)
- Cluster deployment and log orchestration options

Continue to see day 2

Course Breakdown - Day 2:

- Putting It All Together: Threat Hunting with ELK
- Hunting with Windows event logs and Sysmon (free Microsoft Windows endpoint logging tool)
- Hunting with common web server logs and web application logs
- Hunting with and correlating additional log types - syslog, DNS, firewall, IDS/IPS, etc.
- How to search logs to find, analyze, and contextualize anomalous/malicious events using ELK
- How to build and use analytic searches, visualizations, dashboards, automation, and alerting/reporting capabilities
- How to enrich and correlate logs with GeoIP, threat intelligence feeds, ATT&CK mappings, and other log types
- Machine Learning and security analytics
- Capstone: Threat Hunting with ELK CTF Tournament

Minimum computer specs needed for training:

Attendees will use the Intellectual Point comptuers that will have WiFi, 8+ GB RAM, and VirtualBox or VMware installed.

About the Instructor:

Ben brings a diverse background in cybersecurity, IT, law, and law enforcement to Polito. After earning his JD from William & Mary School of Law in 2010 and providing IT and e-discovery support to law firms, Ben joined Booz Allen Hamilton as a cyber security consultant in 2012. While a member of Advanced Persistent Threat (APT) hunt teams assigned to commercial and federal clients, Ben sharpened his network security monitoring, forensics, incident response, malware analysis, cyber threat intelligence, and security architecture skills. He has earned the CISSP, GIAC Certified Forensic Analyst (GCFA), GIAC Web Application Penetration Tester (GWAPT), and Splunk Certified Power User certifications. Ben is a member of the Maryland bar and volunteers at a pro bono legal clinic.

POLITO INC
Masterful Cyber Security