Splunk Enterprise Security Hands-On Workshop

Thank you for attending our Enterprise Security Hands-On workshop. We hope you found it helpful. Below are links referenced during the workshop as well as some other helpful links to use.

Apps Referenced
SA-Investigator for Enterprise Security - https://splunkbase.splunk.com/app/3749/
Enterprise Security Content Update - https://splunkbase.splunk.com/app/3449/
Splunk Stream: https://splunkbase.splunk.com/app/1809/

Additional Data Sources
Splunk Stream:
https://docs.splunk.com/Documentation/StreamApp/latest/User/ConfigureStreams
Osquery: https://osquery.io/
Microsoft Sysmon: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Web Vulnerability Scenario
The Diamond Model of Intrusion Analysis: http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

W3af web vulnerability scanner: http://w3af.org/

WebApp Information Gatherer: https://github.com/jekyc/wig

Exploit Database
- SQL Injection: https://www.exploit-db.com/exploits/40396/
- Cross Site Scripting: https://www.exploit-db.com/exploits/40749/

ES Concepts Covered
- Incident Review:
  http://docs.splunk.com/Documentation/ES/latest/User/IncidentReviewdashboard
- Workflow Actions:
  http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/CreateworkflowactionsinSplunkWeb
- Asset Center:
  http://docs.splunk.com/Documentation/ES/latest/User/IdentityDomaindashboards#Asset_Center_dashboard
- Glass Tables: http://docs.splunk.com/Documentation/ES/latest/User/CreateGlassTable

Commands Used
- stats: https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/stats

APT Scenario
PowerShell Empire: https://github.com/EmpireProject/Empire

Censys.IO: https://censys.io

ES Concepts Covered

Incident Review:
http://docs.splunk.com/Documentation/ES/latest/User/IncidentReviewdashboard
Investigations: http://docs.splunk.com/Documentation/ES/latest/User/Timelines
Adaptive Response Actions:
http://docs.splunk.com/Documentation/ES/5.2.0/User/IncludedResponseActions#Add_threat_intelligence
SSL Search:
http://docs.splunk.com/Documentation/ES/latest/User/ProtocolIntelligence#SSL_Search
Workflow Actions:
http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/CreateworkflowactionsinSplunkWeb

Endpoint/Spyware Scenario
Fruitfly: https://www.blackhat.com/docs/us-17/wednesday/us-17-Wardle-Offensive-Malware-Analysis-Dissecting-OSXFruitFly-Via-A-Custom-C&C-Server.pdf

Updated Information on Fruitfly: https://www.zdnet.com/article/fbi-solves-mystery-surrounding-15-year-old-fruitfly-mac-malware/

Detecting Dynamic DNS Domains In Splunk:
https://www.splunk.com/blog/2015/08/04/detecting-dynamic-dns-domains-in-splunk.html

Device Hunt: https://devicehunt.com

ES Concepts Covered

DNS Search:
http://docs.splunk.com/Documentation/ES/latest/User/ProtocolIntelligence#DNS_Search
Incident Review:
http://docs.splunk.com/Documentation/ES/latest/User/IncidentReviewdashboard
Correlation Searches:
http://docs.splunk.com/Documentation/ES/latest/Admin/Correlationsearchoverview
Lists and Lookups:
http://docs.splunk.com/Documentation/ES/latest/Admin/Createlookups
Endpoint Changes:
http://docs.splunk.com/Documentation/ES/latest/User/EndpointProtectionDomaindashboards#Endpoint_Changes_dashboard

Investigations: http://docs.splunk.com/Documentation/ES/latest/User/Timelines

Hunting with Splunk! Blog Series: https://www.splunk.com/blog/2017/07/06/hunting-with-splunk-the-basics.html

Splunk Quick Reference: https://www.splunk.com/pdfs/solution-guides/splunk-quick-reference-guide.pdf

Splunk Search Reference:
http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/WhatsInThisManual

Additional Resources
Windows Detection and Hunting with Sysmon by Tom Ueltschi:
https://www.first.org/resources/papers/conf2017/Advanced-Incident-Detection-and-Threat-Hunting-using-Sysmon-and-Splunk.pdf

Windows logging configuration cheatsheets: https://www.malwarearchaeology.com/cheat-sheets/

Endpoint Threat Hunting Using Splunk and Sysmon:
https://medium.com/@haggis_m/splunking-the-endpoint-threat-hunting-with-sysmon-9dd956e3e1bd

Forum of Incident Response and Security Teams (FIRST): https://first.org