Security Ninjutsu Part Six @ .conf2019

Slide # to Topic, and Source Material. Go deeper with more detail and documentation!

Slide #	Topic	Location of Source Material
18-20	MITRE ATT&CK in Splunk Security Essentials	Guides will be posted, also covered in SEC2013 at .conf19. Splunk Security Essentials: https://www.splunksecurityessentials.com/
21	Analytics Advisor in Splunk Security Essentials	Announcement Blog Post: https://www.splunk.com/blog/2019/05/15/using-security-essentials-2-4-analytics-advisor.html . Covered in SEC2013 at .conf19. Splunk Security Essentials: https://www.splunksecurityessentials.com/
22	Find New Local Admins	Splunk Security Essentials: "Find New Local Admin" in the app. Docs Link: https://docs.splunksecurityessentials.com/content-detail/showcase_new_local_admin_account/
23	Typo-based Phishing Detection	Splunk Security Essentials: "Emails With Lookalike Domains" in the app. Docs Link: https://docs.splunksecurityessentials.com/content-detail/showcase_emails_with_lookalike_domains/ . Related blog post: https://www.splunk.com/blog/2017/11/03/you-can-t-hyde-from-dr-levenshtein-when-you-use-url-toolbox.html
25	First Time Seen	Ninjutsu Part Five (https://davidveuve.com/splunk.html#ninjutsupartfive) Slides 34-39. Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 108-113. Confidence Checking for First Time Seen Detections covered in Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 85-88.
26	First Time Seen Lookup Caching	Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 79-84
30	Visibility Analysis and Action	Ninjutsu Part One (https://davidveuve.com/splunk.html#ninjutsupartone) Slide 7 (and then throughout the deck)
31	Field Stuffing Technique	New! No other documentation
35-37	Time Series Detections	Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 114-132. Ninjutsu Part Five (https://davidveuve.com/splunk.html#ninjutsupartfive) Slides 60-66
38-41	Excluding Yesterday for Avg w/ Stats+Eval	Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 119-120
42	IQR	Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slide 130. Ninjutsu Part Five (https://davidveuve.com/splunk.html#ninjutsupartfive) Slides 67-70
43	MLTK PDF	Docs Link: https://docs.splunk.com/Documentation/MLApp/4.4.1/User/Algorithms#DensityFunction . There are also examples in ES, and we should provide something clear in the near future.
44	MLTK K-means Clustering with StDev and IQR	Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 156-169. Summarized in Ninjutsu Part Five (https://davidveuve.com/splunk.html#ninjutsupartfive) Slides 71-74
45	StDev based Long Process Detection	Splunk Security Essentials: "Malicious Command Line Executions" in the app. Docs link: https://docs.splunksecurityessentials.com/content-detail/sser_malicious_command_line_executions/
47-60	How does Splunk indexing and search work?	A variety of courses in https://www.davidveuve.com/searchdeepdive/
64-70	How does tstats and Data Model Acceleration	Covered in http://davidveuve.com/splunk.html#tstats
72-73	What is Summary Indexing	Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 69-78. Ninjutsu Part Five (https://davidveuve.com/splunk.html#ninjutsupartfive) Slides 34-39
74	Summary Indexing in JSON	New! Small note in Ninjutsu Part Five (https://davidveuve.com/splunk.html#ninjutsupartfive) Slides 44

75-76	tstats+Summary Indexing All in One "Just the Hits"	Ninjutsu Part Five (https://davidveuve.com/splunk.html#ninjutsupartfive) Slides 41-42
80	SPL Consolidation	Single PDF provided at: http://davidveuve.com/splunk.html#ninjutsupartsix
81-84	Risk Searches	Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 93-98. Some SPL also covered in 37-43
85	Time Series Detections	Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 114-132. Ninjutsu Part Five (https://davidveuve.com/splunk.html#ninjutsupartfive) Slides 60-66
86	Confidence Checks	Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 85-92 (First Time Seen, then Time Series)
88-89	IQR Anomaly (raw and tstats)	Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slide 130. Ninjutsu Part Five (https://davidveuve.com/splunk.html#ninjutsupartfive) Slides 67-70
90-94	Ratio-based Anomaly Detection	Ninjutsu Part Five (https://davidveuve.com/splunk.html#ninjutsupartfive) Slides 56-58
95-97	First Time Seen	Ninjutsu Part Five (https://davidveuve.com/splunk.html#ninjutsupartfive) Slides 34-39. Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 108-113. Confidence Checking for First Time Seen Detections covered in Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 85-88.
98	Examples of other First Time Seen	Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slide 113
99	Peer Group Analysis w/ First Time Seen	Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 110, 112
100	Evaluating Risk of IPS hit based on Signature Frequency	Ninjutsu Part Two (https://davidveuve.com/splunk.html#ninjutsuparttwo) Slides 43-45
101	Alert on Users logging into More than Typical	Ninjutsu Part Two (https://davidveuve.com/splunk.html#ninjutsuparttwo) Slides 30-33
102-104,106	Combining Multiple Data Sources	Ninjutsu Part Two (https://davidveuve.com/splunk.html#ninjutsuparttwo) Slides 14-22
105	Full Ironport Summary Indexing	Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 99-107
107	Superman Analysis (Geo-IP Land Speed Violation)	Splunk Security Essentials: "Malicious Command Line Executions" in the app. Docs link: https://docs.splunksecurityessentials.com/content-detail/land_speed_privileged/
108	Processes with High Entropy Names	Splunk Security Essentials: "Processes with High Entropy Names" in the app. Docs link: https://docs.splunksecurityessentials.com/content-detail/showcase_high_entropy_processes/
109-110	Enrich with Organizational Context and Risk	Ninjutsu Part Four (https://davidveuve.com/splunk.html#ninjutsupartfour) Slides 59-63
112-116	Risk-Based Alerting Intro	Ninjutsu Part Five (https://davidveuve.com/splunk.html#ninjutsupartfive) Slides 75-87 (Contains other Links). Primary among these: https://conf.splunk.com/watch/conf-online.html?search=SEC1479#/. Also this year: https://conf.splunk.com/learn/session-catalog.html?search=risk-based#/
117	JPMC Presentation from .conf2017	.conf Site: https://conf.splunk.com/watch/conf-online.html?search=SCF122584#/
118	American Family Insurance Presentation from .conf18	.conf Site: https://conf.splunk.com/watch/conf-online.html?search=SEC1479#/
123	Splunk Security Essentials	Main Website: https://www.splunksecurityessentials.com . Docs Site: https://docs.splunksecurityessentials.com/ . Splunkbase: https://apps.splunk.com/app/3435
	All of David's Conf Talks	https://www.davidveuve.com/splunk.html