splunk> .conf2017

Threat Hunting with Deceptive Defense and Splunk Enterprise Security

Satnam Singh | Chief Data Scientist
Acalvio Technologies

September 27, 2017 | Washington, DC

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Threat Hunting

- Alert triage using threat intelligence and other data sources
- Primarily outlier detection
- Too many alerts and Too many false positives
- Typically less than 5% of alerts are investigated

" Nearly 45% of Organisations hunt on Ad hoc basis"

SANS Institute, 2017 Report

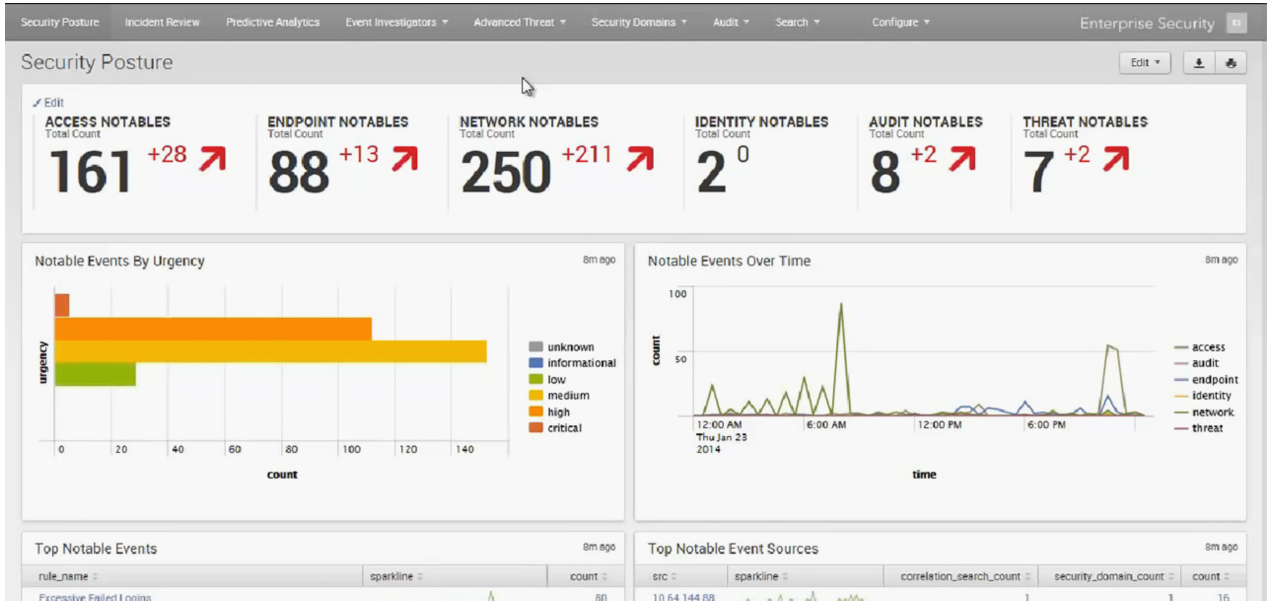
splunk> .conf2017

Deceptive Security

- Reincarnation of Honeypots, Honeyfiles, Honeydata and Honeynet
- Multiple forms : Decoys, Breadcrumbs, Lures, Baits
- Active Approach —> High Fidelity Alert
- “Deploy deceptions on/around hosts with notable events”

Splunk Enterprise Security Notables

- Use Splunk ES Notable Events as Starting and Ending Point
- **Use Data Science** to rank hosts and notable events for hunting

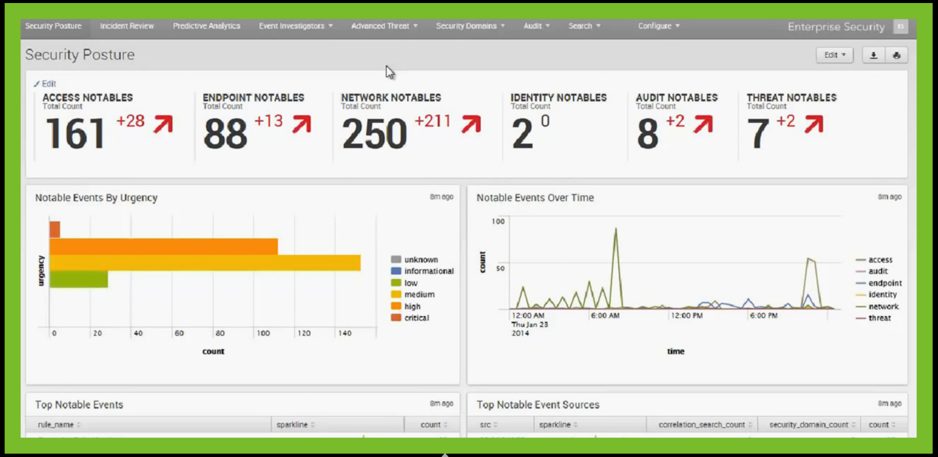


rule_name	sparkline	count
Excessive Failed Logins		80

src	sparkline	correlation_search_count	security_domain_count	count
10.64.144.88		1	1	16

Threat Hunting

Splunk ES -Notables



Security Posture

ACCESS NOTABLES
Total Count
161 +28 ↗

ENDPOINT NOTABLES
Total Count
88 +13 ↗

NETWORK NOTABLES
Total Count
250 +211 ↗

IDENTITY NOTABLES
Total Count
2 0

AUDIT NOTABLES
Total Count
8 +2 ↗

THREAT NOTABLES
Total Count
7 +2 ↗

rule_name	sparkline	count

src	sparkline	correlation_search_count	security_domain_count	count

1. Threat Hunting Intelligence Engine (THIN)

- Ranking of Hosts & Notables
- Determine Deception Strategy

2. Deception Platform

Deploy Deceptions

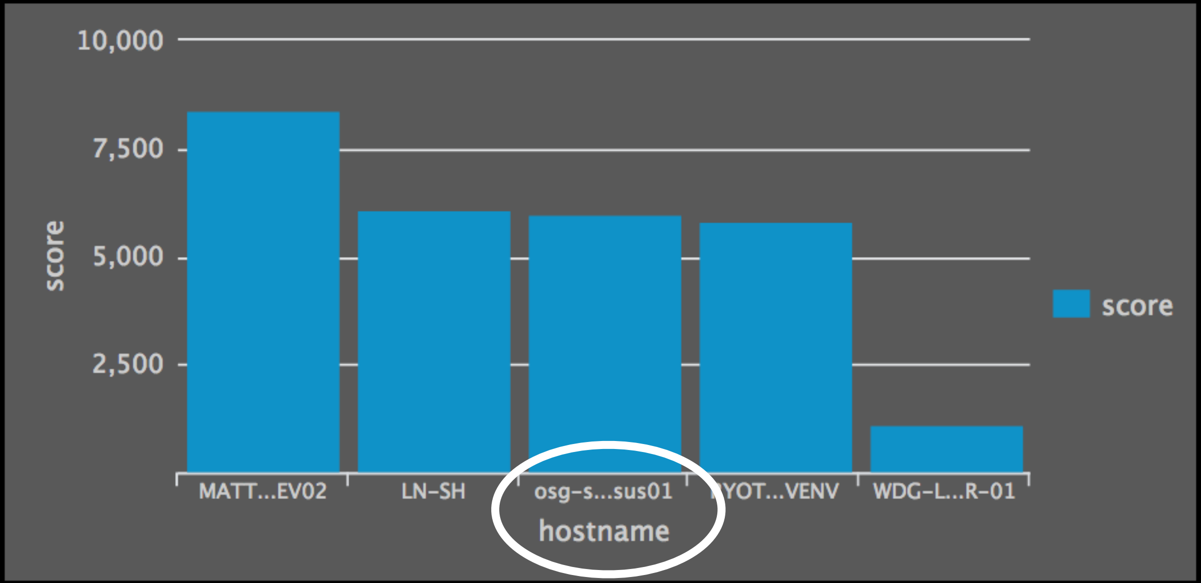
3. THIN

Based on Deception alert/no alert recompute notable ranking

splunk> .conf2017

Step 1: Ranking of Hosts and Notables

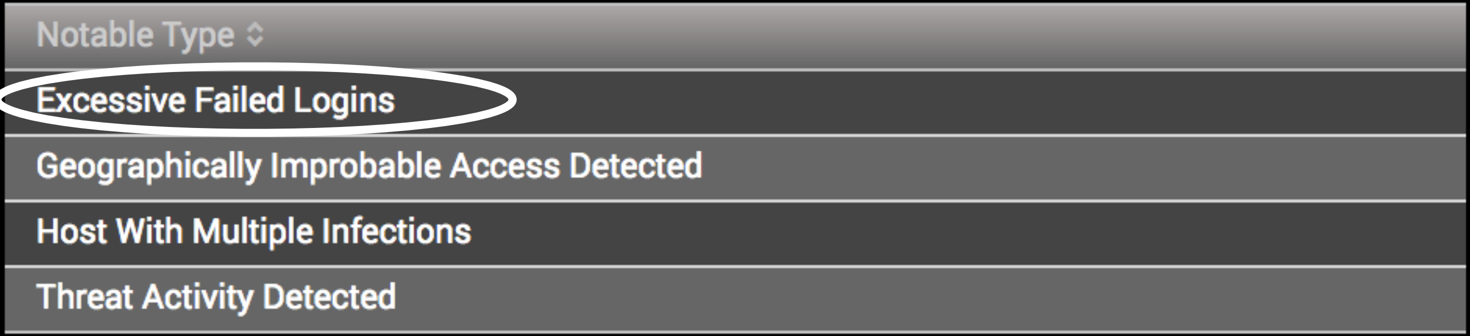
Host Ranking before Deception



Number of Candidate Notables

243

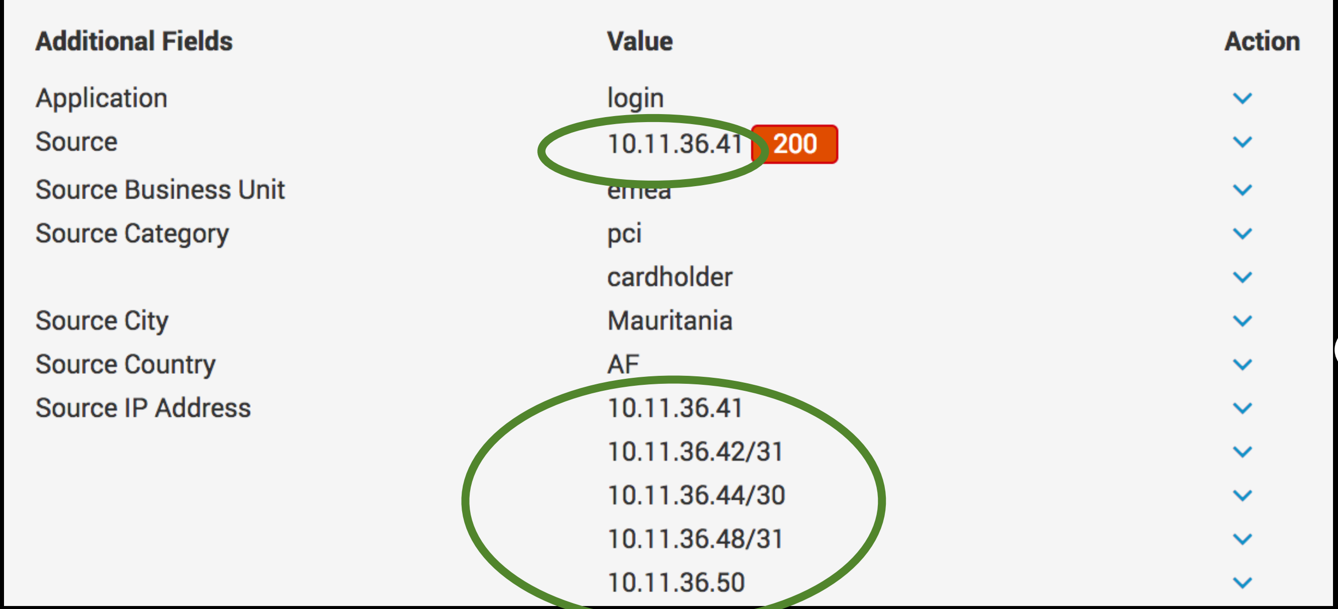
Types of Candidate Notables



Notable Type ⇕
Excessive Failed Logins
Geographically Improbable Access Detected
Host With Multiple Infections
Threat Activity Detected

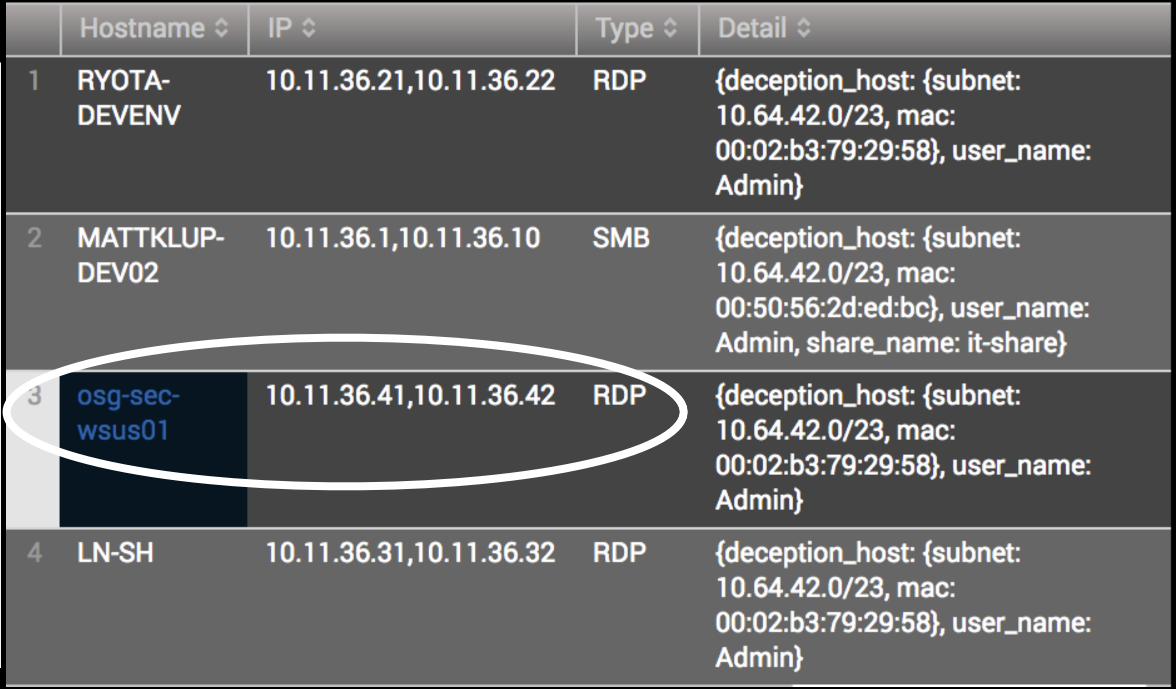
Step 2: Recommend Deceptions

Excessive Failed Logins Notable



Additional Fields	Value	Action
Application	login	⌄
Source	10.11.36.41 200	⌄
Source Business Unit	emea	⌄
Source Category	pci	⌄
	cardholder	⌄
Source City	Mauritania	⌄
Source Country	AF	⌄
Source IP Address	10.11.36.41	⌄
	10.11.36.42/31	⌄
	10.11.36.44/30	⌄
	10.11.36.48/31	⌄
	10.11.36.50	⌄

Breadcrumb Details

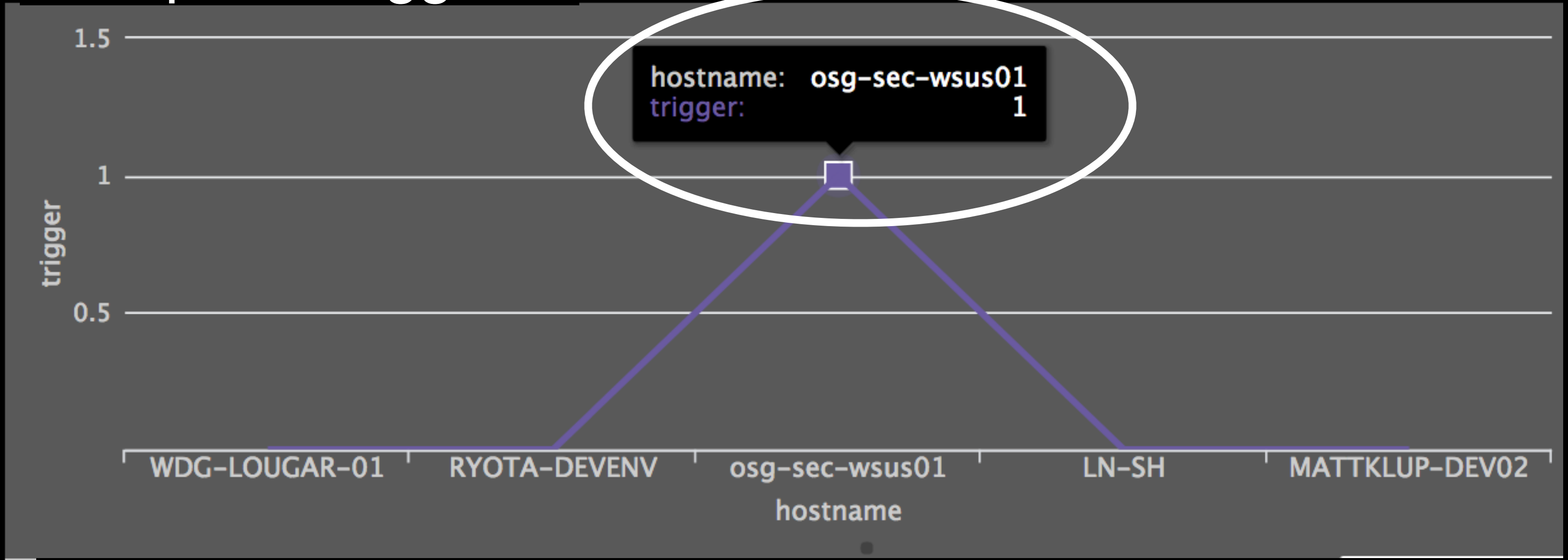


	Hostname ⇕	IP ⇕	Type ⇕	Detail ⇕
1	RYOTA-DEVENV	10.11.36.21,10.11.36.22	RDP	{deception_host: {subnet: 10.64.42.0/23, mac: 00:02:b3:79:29:58}, user_name: Admin}
2	MATTKLUP-DEV02	10.11.36.1,10.11.36.10	SMB	{deception_host: {subnet: 10.64.42.0/23, mac: 00:50:56:2d:ed:bc}, user_name: Admin, share_name: it-share}
3	osg-sec-wsus01	10.11.36.41,10.11.36.42	RDP	{deception_host: {subnet: 10.64.42.0/23, mac: 00:02:b3:79:29:58}, user_name: Admin}
4	LN-SH	10.11.36.31,10.11.36.32	RDP	{deception_host: {subnet: 10.64.42.0/23, mac: 00:02:b3:79:29:58}, user_name: Admin}

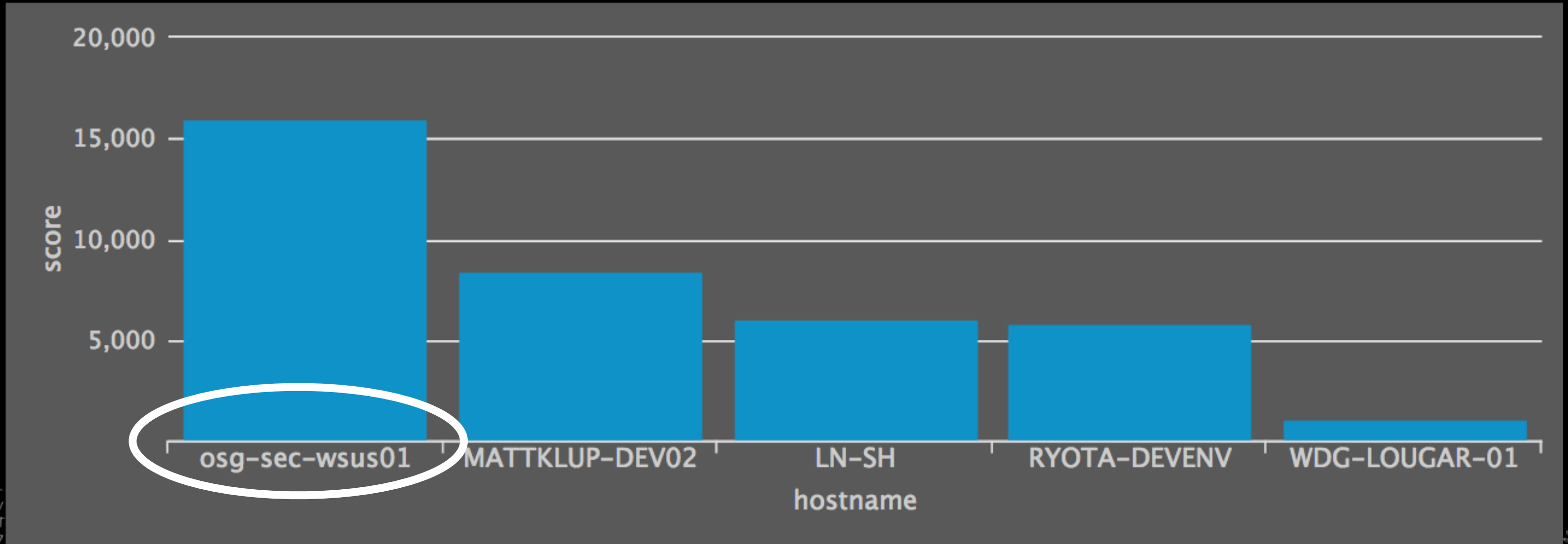
Host osg-sec-wsus01 (10.11.36.41) has failed login authentication 6 times using 6 usernames against 1 target in the last hour

Step 3: Update Ranking using Deception Alerts

Deception Triggered



Updated Ranking based on Deception Alerts



splunk> .conf2017

Summary

- Need to deal with alert deluge
- Need Proactive Approach for Threat Hunting
- Fusion of Data Science and Deceptive Security provides an active approach for Threat Hunting