.conf2015

Full Stack Splunk Development or "How to Build a Splunk Apptitude Winner App"

Mika Borner & Simon Balz

LC Systems

splunk>

Disclaimer

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 the 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.

Agenda

- Team
- Idea
- Implementations
- Architecture
- Challenges
- Final Solution
- Tips 'n' Tricks
- Future

Team

Alert Manager

Mika Borner

- Consultant @ LC Systems
- Splunking since 2006
- Twitter: my2ndhead

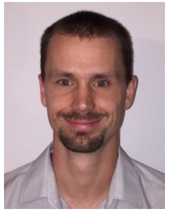
Simon Balz

- Consultant @ LC Systems
- Splunking since 2007
- Twitter: simonbalz

Hyperthreat App Suite (additionally)

Christoph Dittmann

- Consultant @ LC Systems
- Mr. Business Intelligence
- Twitter: mulibu_flyingk



Harun Küssner

- Consultant @ LC Systems
- Mr. Crypto

Idea

Alert Manager

(Category "Innovation")

- Idea born from several customer needs
- Needed a temporary ticketing solution quickly
- Full e-mail white labeling was missing
- QUAD solution at customer was in place
- Wanted to do the "Real Thing"

Hyperthreat App Suite

(Category "Fraud & Insider Threat")

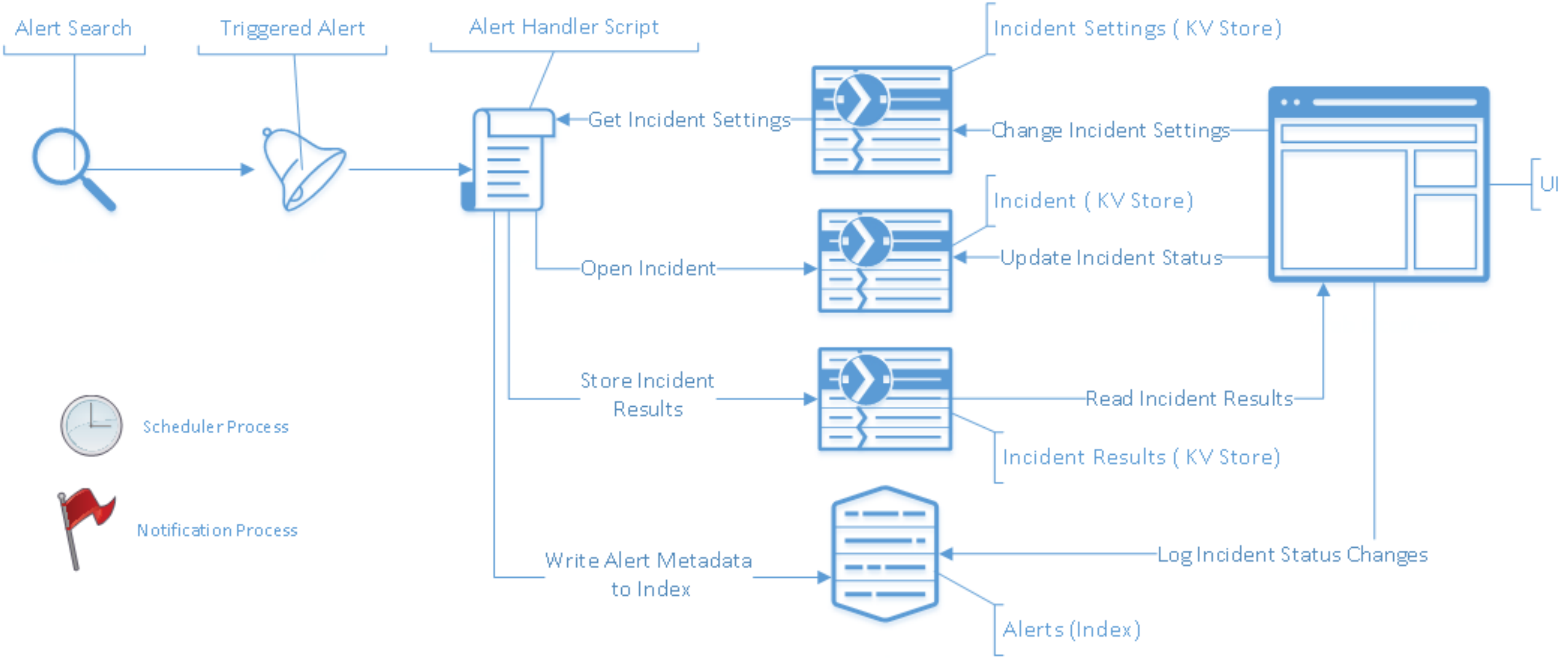
- Apptitude2 provided a DARPA data set with Insider Threat
- Scratching heads for a couple of weeks
- Risk Scoring and Baselining looked like the right approach to solve the challenge
- Employee privacy was a concern. This had to be solved

Implementation

Alert Manager

- **Scripted Alert Action** contains logic to transform an alert into a stateful incident (alert handler)
- KV Store used for storing incident (-state), incident results and incident settings
- Index used to track changes to incidents (audit).
- Lots of UI code for manipulating incident states
- Additional Python code that handles scheduling to close incidents by conditions and to manage notifications

Architecture (Alert Manager)

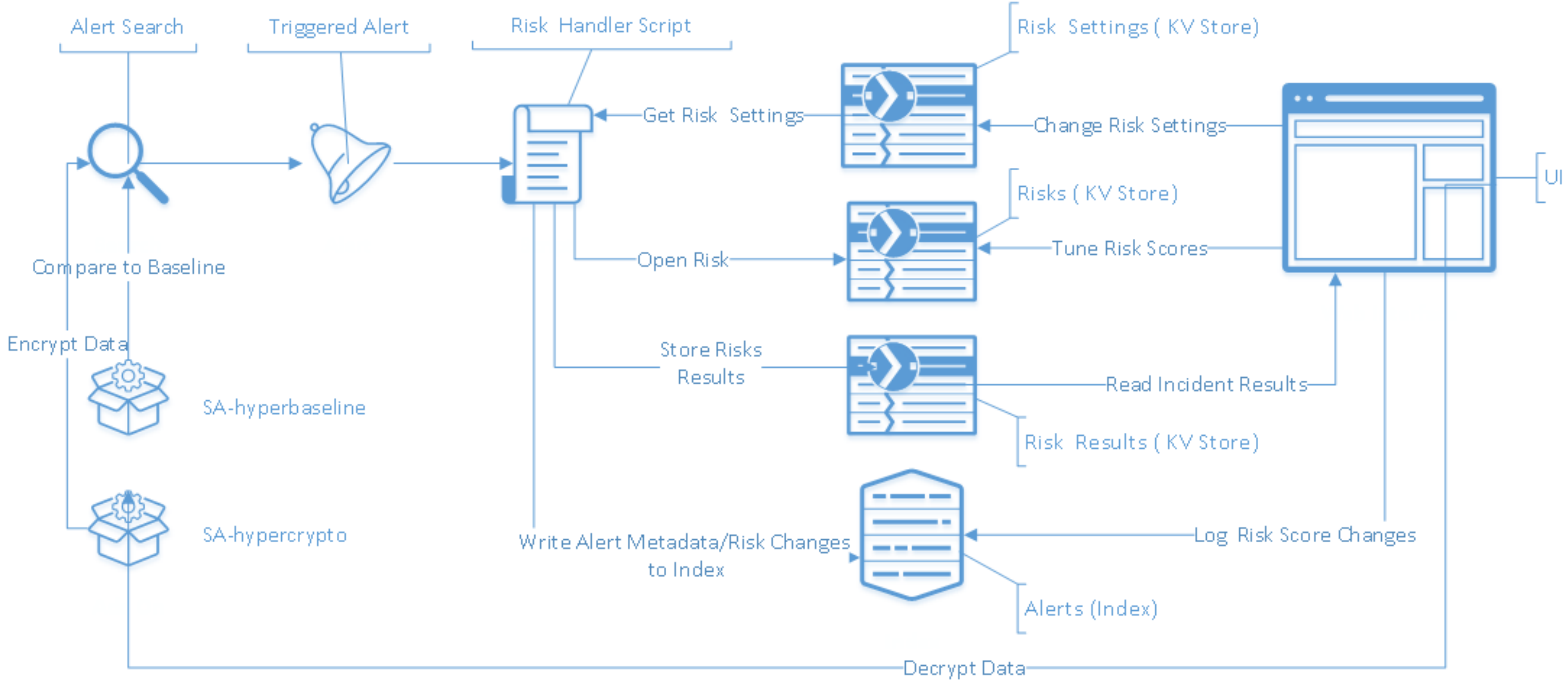


Implementation

Risk Manager

- Risk Manager (App and TA)
  - Alert Script contains logic to look for risk objects and execute scoring
  - KV Store used for storing Risks, Risk Results and Risk Settings
  - Index used to track risk score changes.
  - Lots of UI code for manipulating incident states
- Hyperbaseline (SA)
  - Implemented as custom search command
  - Uses KV-Store to store baseline and read from baseline
- Hypercrypto (SA)
  - Implemented as custom search command
  - Implements hashing algorithms and public key encryption
  - Stores private key pw inside Splunk keystore

Architecture (Hyperthreat App Suite)



Challenges

Alert Manager

- Time (What a surprise… ☺)
- There was no state-of-the-art to manage extended configuration
- Undocumented features like MongoDB filters or Splunk python API
- Fast growth in number of functionalities resulted in spaghetti code
- Full-stack Splunk feature usage: Splunk Web/Splunkd Endpoints, Splunk, Custom search commands, Knowledge objects, Web Stack
- Testing was time-consuming and often done by hand

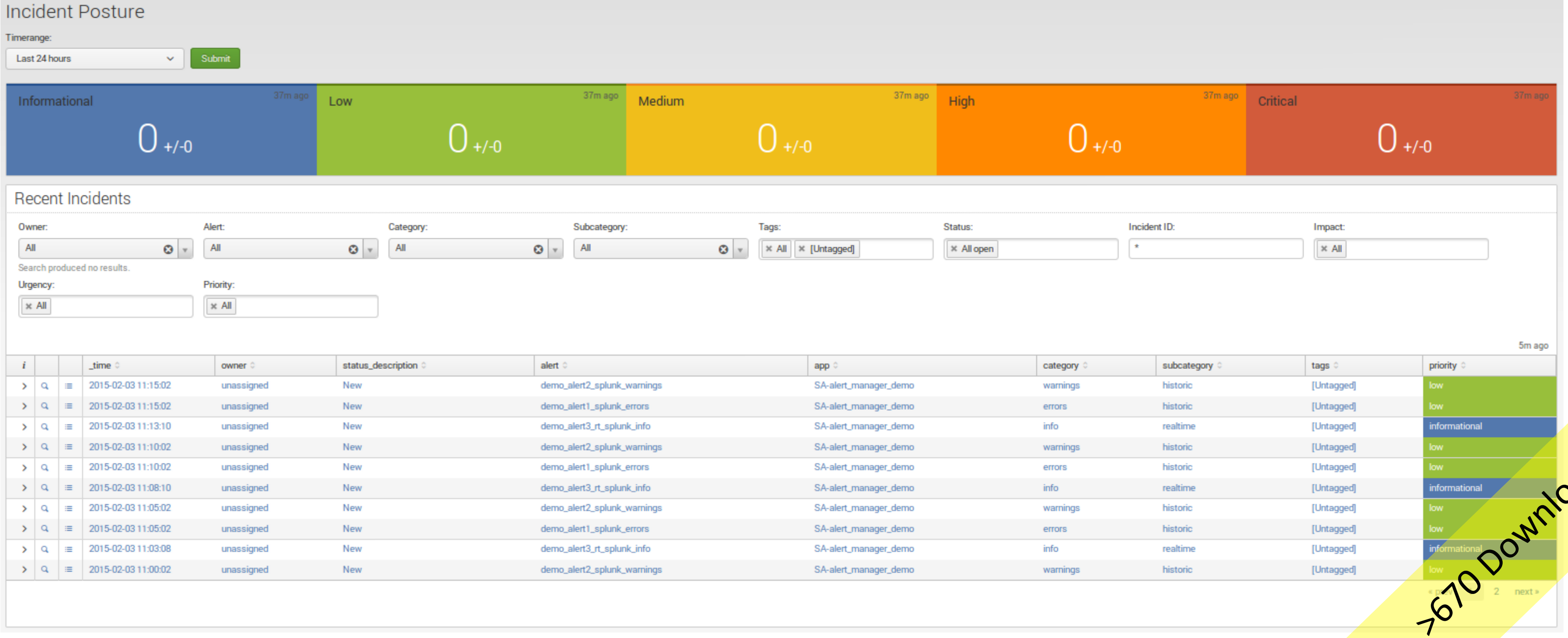
Challenges

Hyperthreat App Suite

- Time (Hit us again ☺)
- Huge (!) DARPA dataset had to be understood first
- Putting it all together in time and hoping it would work
- False assumptions
  - Keystore did not work as we expected
  - Setting up demo environment took longer than expected

Final Solution

Alert Manager @ https://splunkbase.splunk.com/app/2665



Incident Posture

Timerange: Last 24 hours ⌄ Submit

Informational	Low	Medium	High	Critical
37m ago	37m ago	37m ago	37m ago	37m ago
0 +/-0	0 +/-0	0 +/-0	0 +/-0	0 +/-0

Recent Incidents

Owner: All

Search produced no results.

Alert: All

Category: All

Subcategory: All

Tags: × All × [Untagged]

Status: × All open

Incident ID: *

Impact: × All

Urgency: × All

Priority: × All

5m ago

i			_time	owner	status_description	alert	app	category	subcategory	tags	priority
›	🔍	≡	2015-02-03 11:15:02	unassigned	New	demo_alert2_splunk_warnings	SA-alert_manager_demo	warnings	historic	[Untagged]	low
›	🔍	≡	2015-02-03 11:15:02	unassigned	New	demo_alert1_splunk_errors	SA-alert_manager_demo	errors	historic	[Untagged]	low
›	🔍	≡	2015-02-03 11:13:10	unassigned	New	demo_alert3_rt_splunk_info	SA-alert_manager_demo	info	realtime	[Untagged]	informational
›	🔍	≡	2015-02-03 11:10:02	unassigned	New	demo_alert2_splunk_warnings	SA-alert_manager_demo	warnings	historic	[Untagged]	low
›	🔍	≡	2015-02-03 11:10:02	unassigned	New	demo_alert1_splunk_errors	SA-alert_manager_demo	errors	historic	[Untagged]	low
›	🔍	≡	2015-02-03 11:08:10	unassigned	New	demo_alert3_rt_splunk_info	SA-alert_manager_demo	info	realtime	[Untagged]	informational
›	🔍	≡	2015-02-03 11:05:02	unassigned	New	demo_alert2_splunk_warnings	SA-alert_manager_demo	warnings	historic	[Untagged]	low
›	🔍	≡	2015-02-03 11:05:02	unassigned	New	demo_alert1_splunk_errors	SA-alert_manager_demo	errors	historic	[Untagged]	low
›	🔍	≡	2015-02-03 11:03:08	unassigned	New	demo_alert3_rt_splunk_info	SA-alert_manager_demo	info	realtime	[Untagged]	informational
›	🔍	≡	2015-02-03 11:00:02	unassigned	New	demo_alert2_splunk_warnings	SA-alert_manager_demo	warnings	historic	[Untagged]	low

« prev 1 2 next »

>670 Downloads

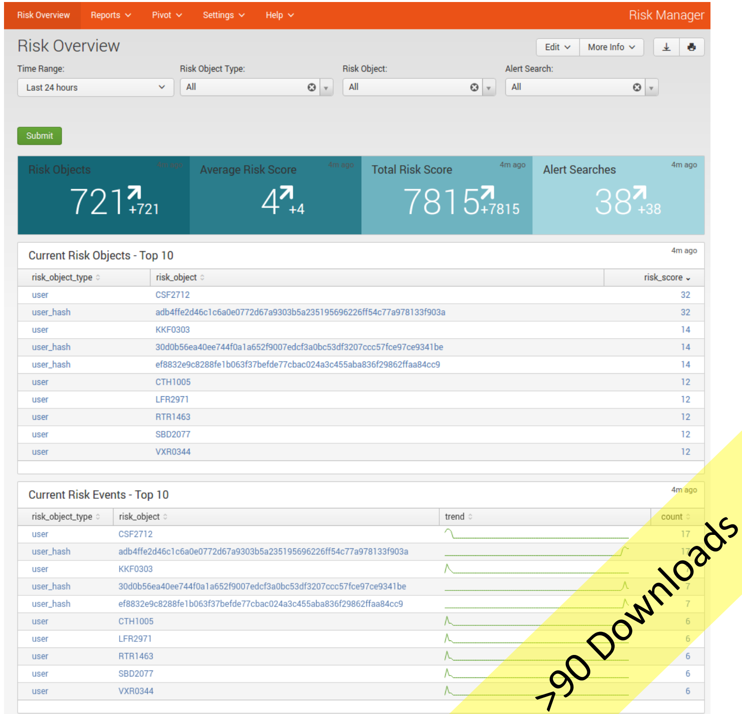
Final Solution

Hyperthreat App Suite

- Risk Manager
  https://splunkbase.splunk.com/app/2804/

- Hyperbaseline
  https://splunkbase.splunk.com/app/2802/

- Hypercrypto
- https://splunkbase.splunk.com/app/2801/



Risk Overview

Time Range: Last 24 hours

Risk Object Type: All

Risk Object: All

Alert Search: All

Risk Objects (4m ago)	Average Risk Score (4m ago)	Total Risk Score (4m ago)	Alert Searches (4m ago)
721 +721	4 +4	7815 +7815	38 +38

Current Risk Objects - Top 10 (4m ago)

risk_object_type	risk_object	risk_score
user	CSF2712	32
user_hash	adb4ffe2d46c1c6a0e0772d67a9303b5a235195696226ff54c77a978133f903a	32
user	KKF0303	14
user_hash	30d0b56ea40ee744f0a1a652f9007edcf3a0bc53df3207ccc57fce97ce9341be	14
user_hash	ef8832e9c8288fe1b063f37befde77cbac024a3c455aba836f29862ffaa84cc9	14
user	CTH1005	12
user	LFR2971	12
user	RTR1463	12
user	SBD2077	12
user	VXR0344	12

Current Risk Events - Top 10 (4m ago)

risk_object_type	risk_object	trend	count
user	CSF2712		17
user_hash	adb4ffe2d46c1c6a0e0772d67a9303b5a235195696226ff54c77a978133f903a		17
user	KKF0303		[illegible]
user_hash	30d0b56ea40ee744f0a1a652f9007edcf3a0bc53df3207ccc57fce97ce9341be		7
user_hash	ef8832e9c8288fe1b063f37befde77cbac024a3c455aba836f29862ffaa84cc9		7
user	CTH1005		6
user	LFR2971		6
user	RTR1463		6
user	SBD2077		6
user	VXR0344		6

>90 Downloads

Tips'n'Tricks

- It's all about the idea!
- Keep it generic
- KV Store is the key to complex apps
- Pretty and complex UI's may require JS/CSS skills. Team up with someone who knows web development
- Read the Splunk Developer Guidance (Lots of gems!)
- Think before code (begin with mockups and a SAD)

Future

Alert Manager / Hyperthreat App Suite

- Documentation
  - Moving from GitHub Wiki to Ponydocs
- Automated Testing
  - With more and more features, we want to keep the quality high
  - Unit Testing needs to be evaluated
- Support
  - Several inquiries about support
  - Growing number of active installation will drive this
- Features
  - Implementing roadmap features
  - Looking into managing all external RFEs

THANK YOU