

Automated Cybersecurity Actions Using Splunk

Recruit Technologies

Mitsuhiro Nakamura | Senior Security Engineer
September 26, 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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

Agenda

This is a short session.

1. BIO
2. Heuristic Analysis with SPL
3. Threat Profiling using Data Visualization
4. Real World
5. Unmanned Defense System
6. Wrap Up

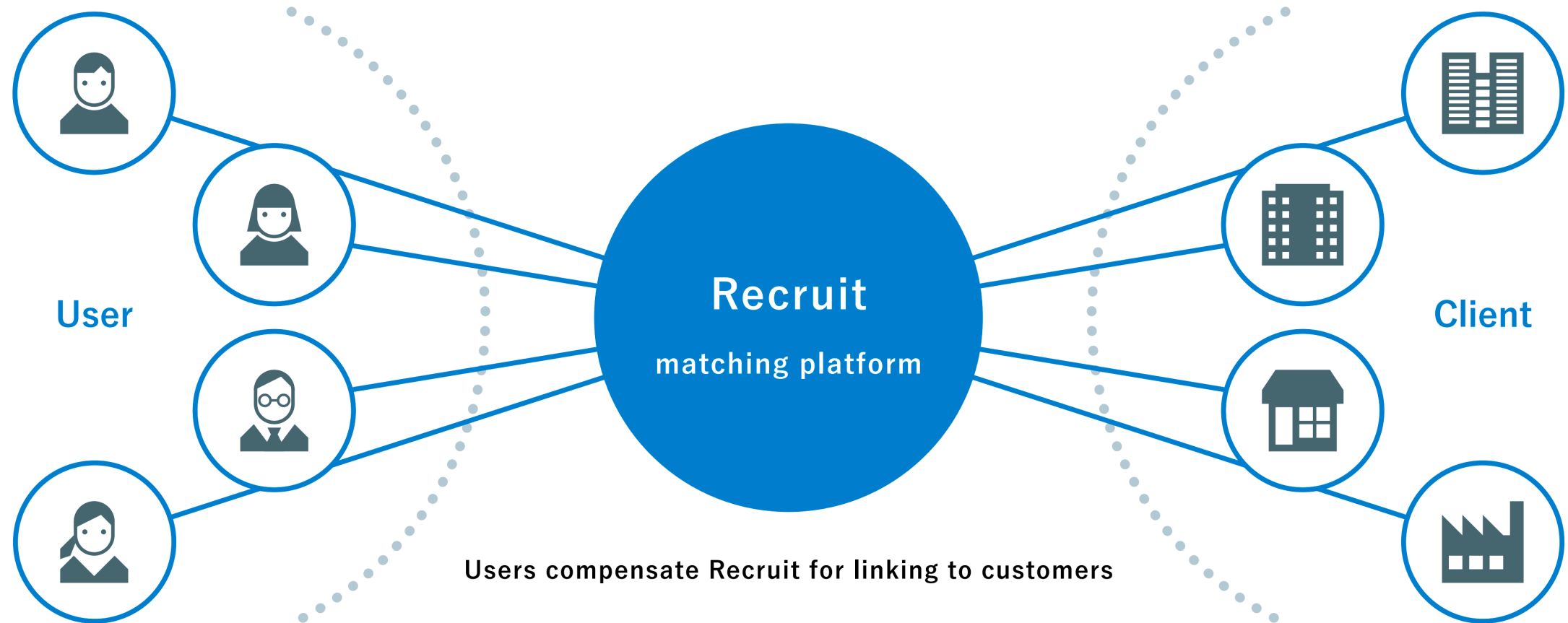
Bio

Mitsuhiro Nakamura (Hiro)

- ▶ 10+ years experience in cyber security specializing in Pen-Test, Forensics, and Incident-Response.
- ▶ Built web application vulnerability assessment methodology.
- ▶ Data analysis for Threat Detection using Splunk.
- ▶ I have gave lectures at conf 2016 (Florida) , and at SplunkLive 2016 (Japan)
- ▶ like : Windsurfing (Wave!)



Business Model



We are committed to creating chances to discover “Opportunities for Life,” connecting users and clients through new channels.

Ref: http://www.recruit.jp/ca_files/annual_2016_all_en.pdf

6





Dig, dig, dig.
Chew this iron bitch up.

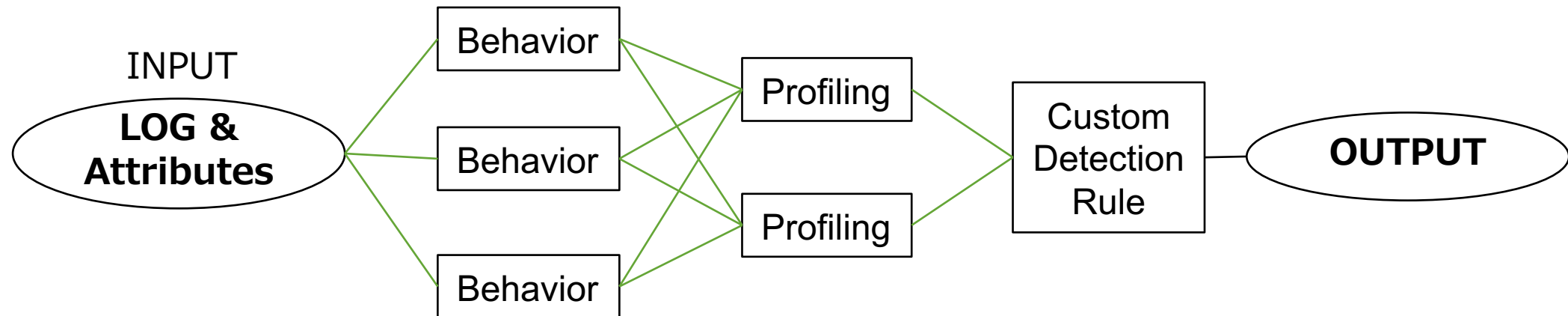
Heuristic Analysis

Recovering Behavior from fragmented data.



Lookup: iplocation / dnslookup / Tor-exitnode /Account Attributes & FingerPrint

▼ SPL (Heuristic)



Behavior

① Building Base Query (Summary Index)

Whois, TorExitNode, WebAPI, etc

Reverse DNS
Country

Log

Auth-DB

Tomcat

Web

● Recovering Behavior per User

Retry Auth-Num (per browser) ReverseDNS

Standard Deviation Intelligence Results

Interval Success-Rate FingerPrint Country

Action User-Attributes Valid ID Numbers

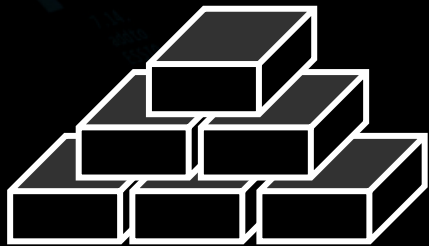
Account Attributes

FingerPrint

② Heuristic Analysis

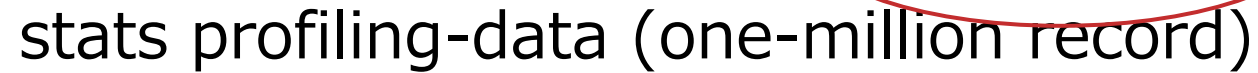
AnomaryData + Attributes + Statistics + StDev + NextStep-Behavior

We use various data before and after the point of incident, plus, User-Attributes.



Threat Profiling

Using Data Visualization

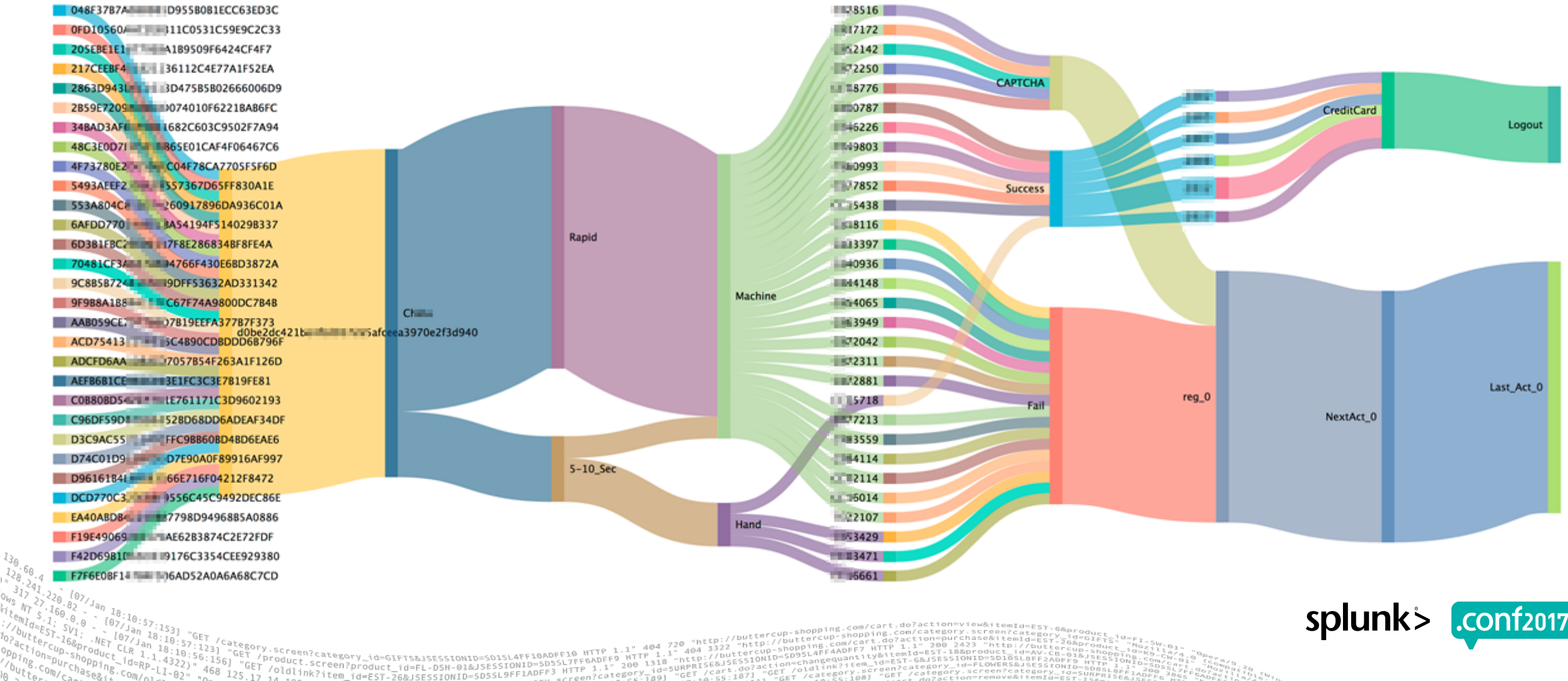


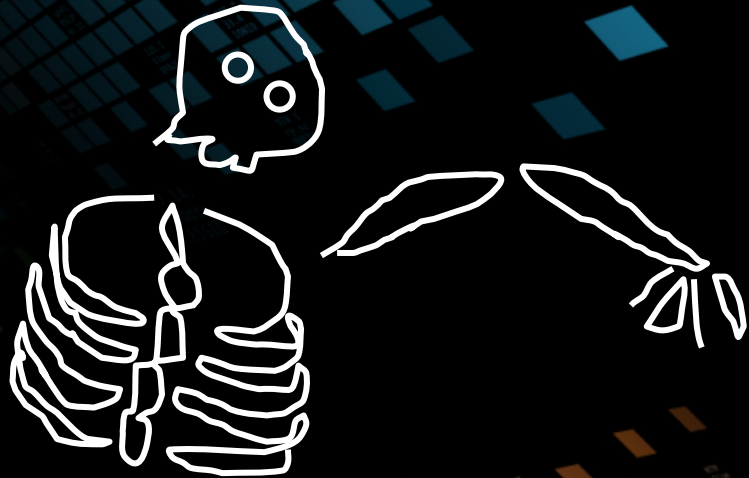
	db_item	db_skuip	db_skuid	db_fukusaka	db_listid	count	st_purchase	City	min_time	max_time	Address/back	shop	db_ZIP	sum_totalItemPrice	sum_GrandPoints	v_ref_shop
	4091	0405	0400	1700	7	9011	9011		03/01 07:31	03/00 23:02		bookben	0400	10174408	111290	bookben
	16	0306	1208	2017	1273	1273	1273		03/01 07:36	03/00 23:02		shochukan	0202	620184	40322	shochukan
	019	015	0409	1309	0	0408	0408		03/01 07:39	03/00 23:02		funy/hondai	06	409906	44906	funy/hondai
	22	09	07	06	0	06	06		03/01 19:25	03/00 23:06		oricauto	6	944501726	112122	oricauto
	124	4074	0204	11	14	0704	0704		03/01 06:33	03/00 23:06		bookunomatsubakaya	3066	2741189	14626	bookunomatsubakaya
	460	2305	2310	0	0	2725	2725		03/01 10:00	03/00 23:06		grape-market	134	3071806	22444	grape-market
	11	200	202	0	1	312	312	21129.216	03/01 04:07	03/00 23:06		cym-machibouken	31	303383	186	cym-machibouken
	24	27	76	7	79	79	79		03/06 22:32	03/00 23:42		hungen	3	138111	581	hungen
	208	021	043	7	1	090	090	2656874.493	03/01 11:40	03/00 23:04		asa-shop	40	627111	27006	asa-shop
	361	023	013	7	0	0417	0417		03/01 06:57	03/00 23:40		benkyo	47	1443487	23962	benkyo
	9	0	7	6	0	0	0		03/03 14:06	03/00 08:43		shinohanger	1	13004	0	shinohanger
	441	2117	2104	6	1	2600	2600	440005.901	03/01 07:06	03/00 23:13		coscoshouse	296	10907078	109681	coscoshouse

Pipeline for Real-Threat Detection

Browser

FingerPrint- FingerPrint - Country - Speed - Bot/Hand - AccountID - Results - Attributes - Action- LastAction





Real World

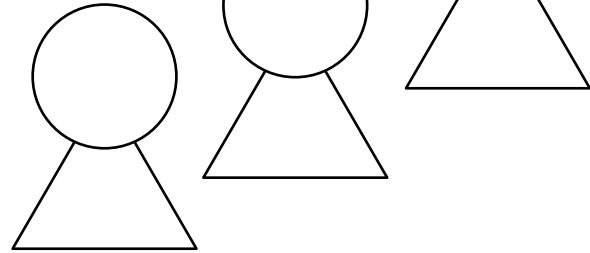
The real aim of the attacker

They Are Coming On The Great Friday Night

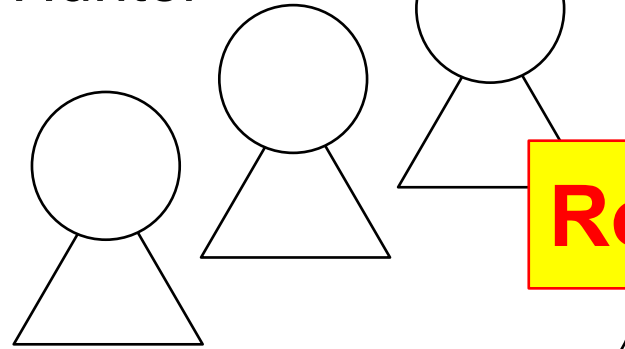
Web

Insider

Attacker



Hunter



Attack

DRUM

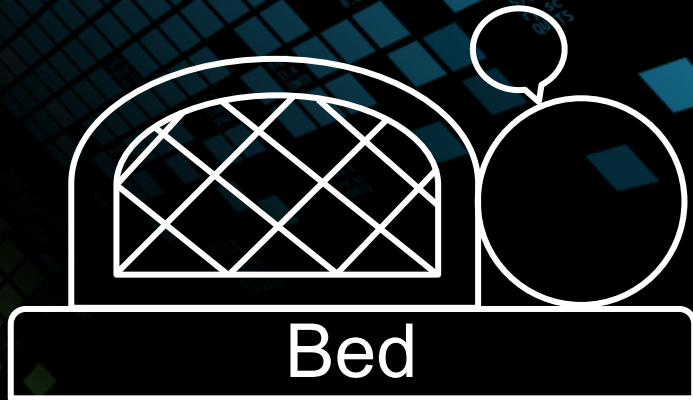
Splunker

Splunker

Splunker



Round 2!! (eternally)



Unmanned Defense System

We call them “Shield”.

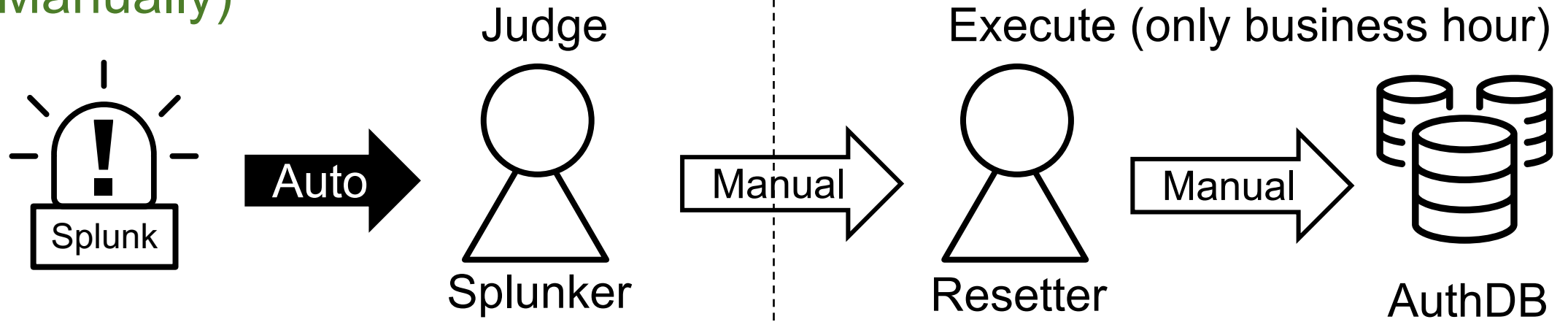
The Birth of Unmanned Defense System

Detection

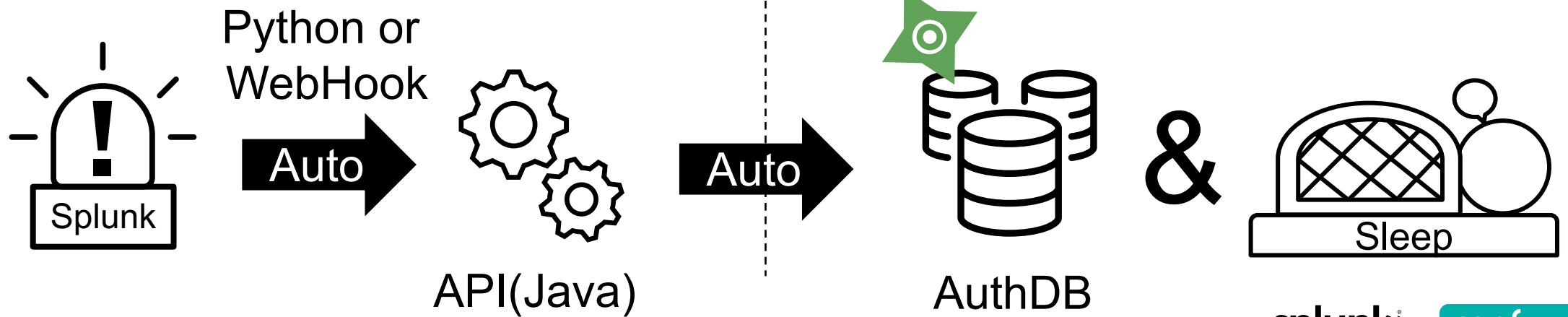
Triage

Respond




Before (Manually)



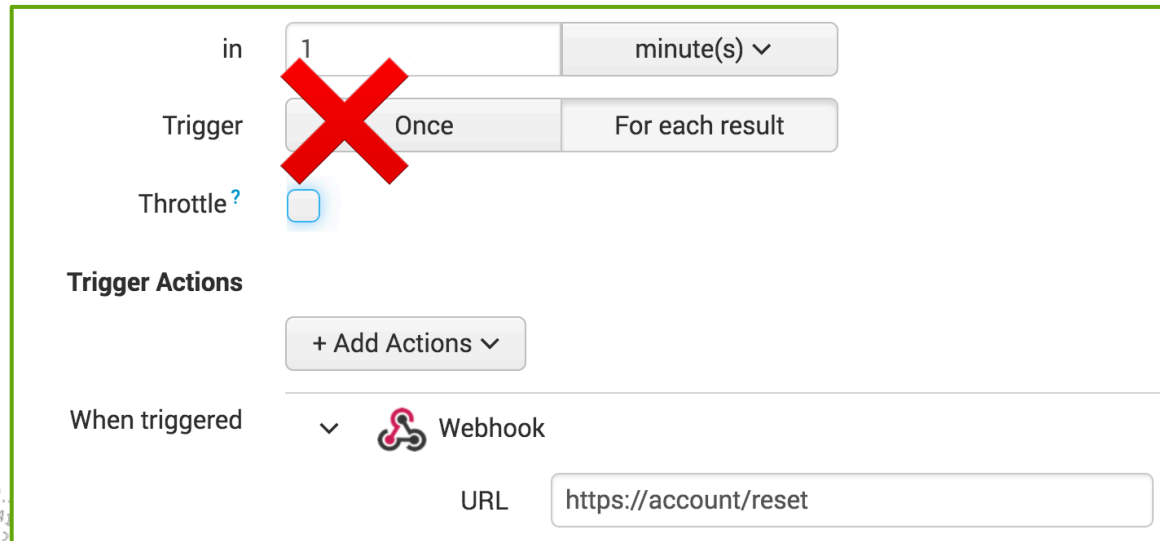
After (Unmanned Defense System)



WebHook vs InterSplunk

Approach	Develop	Format	Multiple	Best Choice
► Webhook	a little 	Solid	Incompatible	JSON, per record
► InterSplunk	Necessary	Flexible 	Supports 	without JSON, Per record or Multiple

WebHook




in 1 minute(s) ▼

Trigger Once For each result

Throttle? ☐

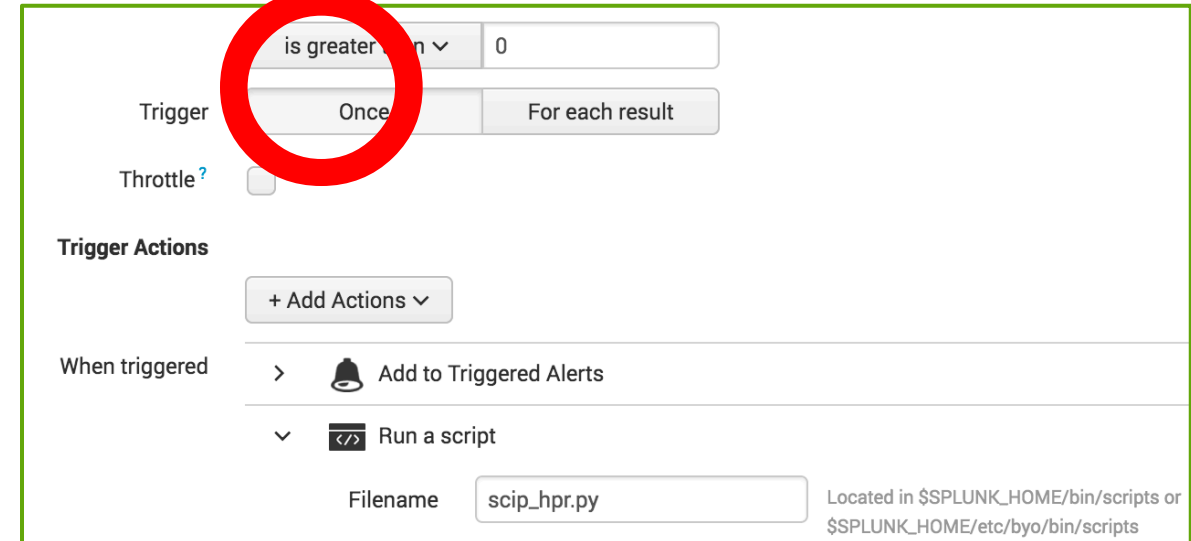
Trigger Actions

+ Add Actions ▼

When triggered ▼  Webhook

URL https://account/reset

Intersplunk(custom alert)




is greater than ▼ 0


Trigger Once For each result

Throttle? ☐

Trigger Actions

+ Add Actions ▼

When triggered >  Add to Triggered Alerts

▼  Run a script

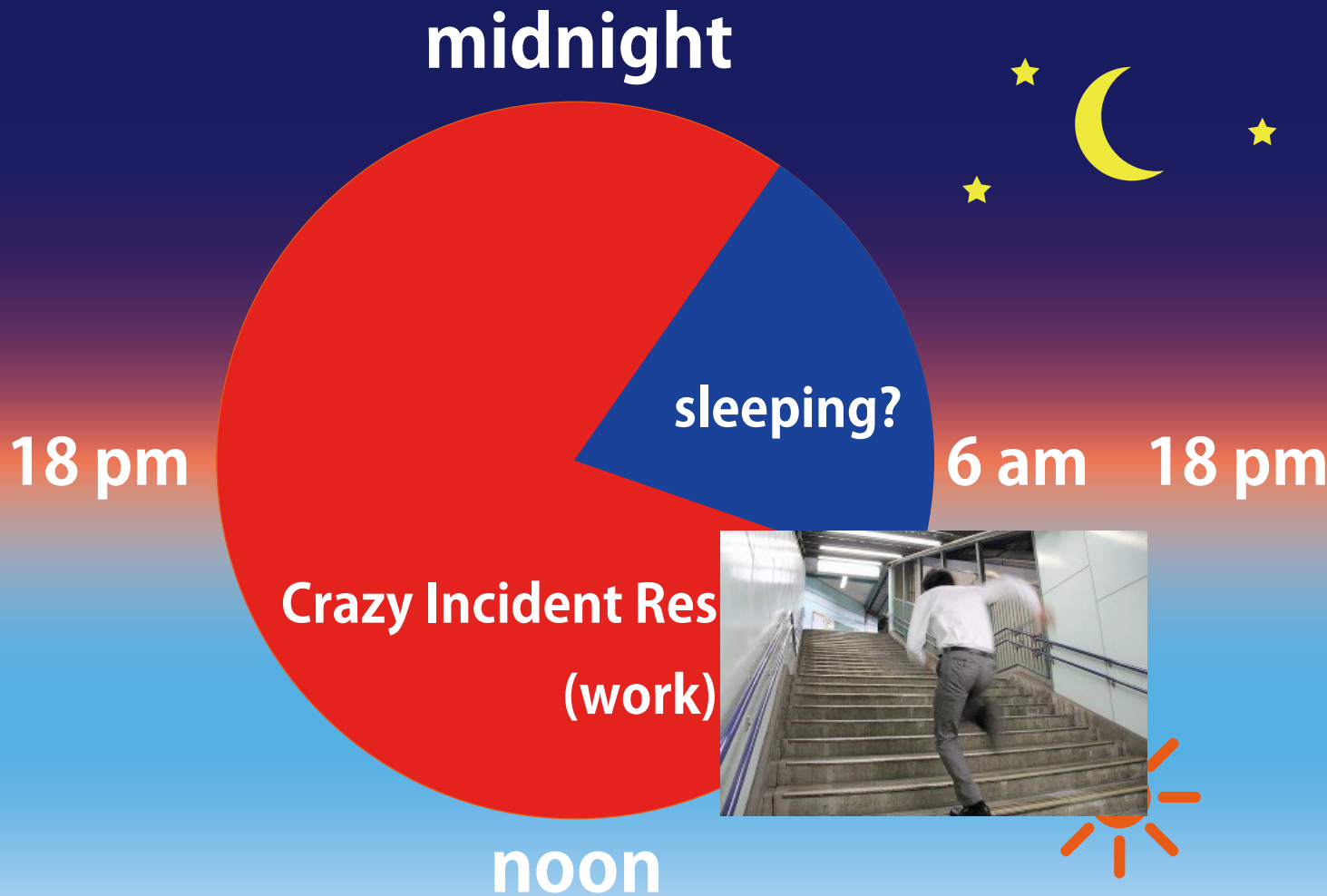
Filename scip_hpr.py

Located in \$SPLUNK_HOME/bin/scripts or \$SPLUNK_HOME/etc/byo/bin/scripts

Comparison

Manually Defense

With Unmanned Defense





Wrap Up

Splunkers for the Future

21



Splunkers for the Future

Task

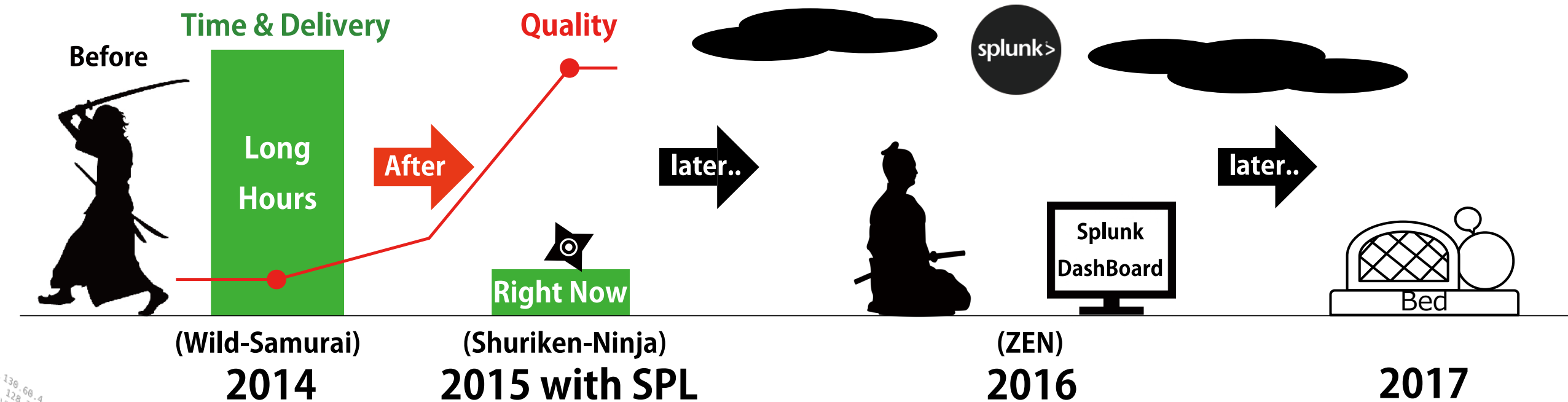
**Automated Action
& Machine Learning**

Human

Innovation

Their DeepAnalysis has changed dramatically.

They can judge things calmly..



Thank You

Facebook : <https://www.facebook.com/hiro.goahead>

Hiro : <nakamura@r.recruit.co.jp>

Don't forget to **rate this session** in the
.conf2017 mobile app

splunk® .conf2017