

Catching Rogue Traders

How a multinational bank used Splunk to catch rogue traders in financial markets

Aleksey Eremenko | Vincent Leycuras

September 2017 | Washington, DC

splunk

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.

About Us

Aleksey Eremenko (Lex)

Background for financial markets & data science

Screen?product id=FL-DSH-01&JSE

- Markets Surveillance
- Think of me as a secret agent

Vincent Leycuras

- Background in financial markets
- Eager to fix the divide between Technologists and the rest of the world
- Splunk convert since 2015





Why We Do What We Do

UBS Rogue Trader Scandal

In early September 2011, the Swiss bank UBS announced that it had lost around 2.3 billion dollars, as a result of unauthorized trading performed by a director of the bank's Global Synthetic Equities Trading team in London.

Societe Generale Rogue Trader

SocGen revealed that in January 2008 that a rogue trader had <u>lost the bank £3.7bn</u>. The trader, had been taking unauthorised positions on stock futures. The trader had previously worked in compliance, and bank bosses suggested he was adept at hiding his losses and bypassing checks.

Baring's Bank Goes Bust

Leeson did make Barings vast sums. In 1993, he made £10m - 10% of the bank's profits for that year. But in 1995, the discovery of a secret file - Error Account 88888 - showed that Leeson had gambled away <u>£827m</u> in Barings's name and the city's oldest merchant bank, and banker to the Queen, went bust.







"Why is it so hard to catch rogue traders?"



Rogue Trader Tactics & Behaviors

Search Quotes, News & Video 🛛 🔍

HOME INTL V NEWS MARKETS INVESTING TECH MAKE IT VIDEO SHOWS MORE

NETNET

Rogue Trading: A How-To Guide



duct.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9



- 1. Get a job on a trading desk
- 2. Trade things your bosses don't understand
- 3. Trade away from the home office
- 4. Know the back office systems
- 5. Trade with other people's accounts
- 6. If you lose money, double down
- 7. Cross your fingers
- 8. Enlist your colleagues
- 9. Confess and point fingers

<u>Need to correlate many non-traditional</u> <u>data sources across multiple systems</u>

splunk>

CONf2017

The Banking Technology Challenge

- Legacy banking infrastructure
- Systems were not designed to accept the granularity of data requirements of today
- Siloed systems & data sources

Creen?product id=FL-DSH-01&JSESS







Enter Splunk!



Our Splunk Story

Developed an app to conduct real-time financial markets monitoring, analytics, reporting & investigations.



Where It All Started

- Technology needed better systems monitoring capability the brief was:
- Ability to monitor flows across systems, not just the systems
- Reuse/recycle legacy tools/scripts/daemons, avoid throw away
- Remove the need for direct server access, especially for non-support staff
- Discovered Splunk almost by accident:
- A project team had sneaked it in for their own needs
- Just enough license headroom to add another system (mine!!)
- Very little exposure, so plenty of opportunity to investigate (i.e., muck around)
- Let the platform grow organically (for a while...)
- More systems were added with virtually 0 marginal cost
- Funding eventually came to build it properly
- All key systems are now on-boarded, the journey really begins NOW







Climbing The Value-Add Ladder

- ► From System Monitoring...
- Financial systems are fault-tolerant, true system failures are rare...
- ▶ ... But integration is extremely hard to get right
- ► → Splunk allows us to measure cross-system efficiency
- ... To Operational Intelligence
- Integration patterns are asynchronous, this can cause choke points and chain reactions...
- ... Often caused by an upstream system
- Splunk allows us to detect early symptoms and contain the risk of outage
- To Trade Surveillance
- Splunk captures all the trade booking steps down to the millisecond
- Which allows for indisputable timelines...

screen?product id=FL-DSH-01&J

🖈 That can be tested against known suspicious patterns





splunk>

Alerts Inbox	Query 🗸	nvestigate 🗸 🛛 Too	ls ∽ Reports ∽	Alerts Case Manage	ment Settings ~ Help	Ý						m s т (•)
Alerts II Current numbe Timerange: Date time ra	er of alerts, trend ov	er selected timerange a	nd list of alerts Hide Filters						Alert	s Inbox		Edit Export ~
		ational		D d Benchmar			Practices	-	2 - 4 Rogue Trading	_,		9 ipulation
Recent Al	lerts											
Owner:		Alert:		Category:	Subcategor	y:	Tags:	Status:		Incident ID:		
All	€	All	٢	* All	All	♥	× All × [Untagged]	× All open		*		
Title:		Impact:		Urgency:	Priority:		Freeform Filter:					
i	_time 0	own	er 0	status_description 0	title 🗘	catego	ıry ≎	Desk 0	Location 0	tags ≎	OutsideHours 0	priority 0
> Q	≡ 2017-05-05	02:15:19.900 L m	istinbox	New	Front Running - F	K Rogue	Trading	FX	New York	[Untagged]	false	medium
> Q	≔ 2017-05-05	02:15:04.839 👤 🖍	stinbox	New	Front Running - F)	K Rogue	Trading	FX	New York	[Untagged]	false	medium
> Q	≔ 2017-05-05	00:25:08.255 📃 👤 n	istinbox	New	Spoofing - Futures	Market	t Manipulation	Commodities	London	[Untagged]	true	medium
> Q	≔ 2017-05-04	18:25:33.345 1 m	astinbox	New	Spoofing - Futures	s Market	t Manipulation	Commodities	Australia London	[Untagged]	false	medium
> Q	≔ 2017-05-04	18:25:28.727 👤 🖍	istinbox	New	Spoofing - Futures	Market	t Manipulation	Commodities	Australia	[Untagged]	false	medium
> 9	≔ 2017-05-04	18:25:23.179 👤 🖍	istinbox	New	Spoofing - Futures	Market	t Manipulation	Commodities	Australia	[Untagged]	false	medium
> Q	≔ 2017-05-04	18:25:18.555 L m	istinbox	New	Spoofing - Futures	Market	t Manipulation	Commodities	Australia	[Untagged]	false	medium
> Q	≔ 2017-05-04	18:25:09.959 👤 🖍	istinbox	New	Spoofing - Futures	Market	t Manipulation	Commodities	Australia	[Untagged]	false	medium
	≔ 2017-05-04			New	Spoofing - Futures		t Manipulation	Commodities	Australia	[Untagged]	false	medium
~ Q	≔ 2017-05-04	14:25:13.590 L m	stinbox	New	Spoofing - Futures	Market	t Manipulation	Commodities	Australia	[Untagged]	false	medium
inci His	story time ≎	56ed-4598-a2f3-52bb54 user 0	id798fe) impact= <mark>medi</mark>	um urgency= medium	action 0	details 0	co	mment 0				
s NT 27.220.82 s NT 5.1; 50.0 temid=EST.1600 voutercup.sho ping.com/cha	7/Jan 18:10:57:15 0 - (07/Jan 18:1 0 - NE (07/Jan 18:1 0 - NE (07/Jan 18) 0 - NE (07/Jan	3] "GET /category. 9:57:123] "GET /pr 10:56:163] "GET / 322)" 468] "GET /	Screen?category_id Dduct.screen?produ Ddlink?item id==c	=G1FT5&15E5510N1D=5015 ct_id=FL=D5H=01&25E551 T_oce_ecctroutD=cfs519	LAFF19ADFF10 HTTP 1.1" 404 ONID=SD55L7FF6ADFF9 HTTP 1. ONID=SD55L7FF6ADFF9 HTTP 1.1" 200 JT FFIADFF3 HTTP 1.1" 200 JT recent2ctesc77.ad	720 "http://buttercup- 1" 404 3322 "http://bu "http://buSSIONID=SD SURPRISE&JSESSIONID=SD "cET /cartiga]	<pre>ihopping.com/cart.do?actic itercup-shopping.com/cate ping.com/cart.do?actic ping.com/cart.do?actic ping.com/cart.do?actic com/cart.do?actic com/cate&profile /cate≺</pre>	on=view&itemId=EST-6&p gorriscreenzcategory 2423 ***********************************	00000000000000000000000000000000000000	^π ^π Ω ^φ Ω	splunk>	.conf2017





Trend Reporting & Drilldown Analytics









Alerts by Trader

Jan

10:57:153] (07/Jan

id≈RP.

.4322) 468 126 17 14 44





Alerts by Type





shopping.com/cart.do?action=view&itemId=E5T-6& "/133] "GET /category.screen?category_id=GIFTS&LSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping cc 1.1:10:56:156] "GET /product.screen?product_id=GIFTS&LSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 404 3322 "http://buttercup-shopping cc 1.1:4322) "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SDSSL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping cc (num_02) "GET /oldlink?item_id=EST-26&JSESSIONID=SDISLAFF10ADFF10 HTTP 1.1" 200 1318 "http://buttercup-shopping (num_02) "GET /oldlink?item_id=EST-26&JSESSIONID=SDISLSSIONID=SDISL7FF6ADFF9 HTTP 1.1" 200 1318 "http://act.do?arcfor.org (num_02) "GET /category_id=SUF_26&JSESSIONID=SDISL9FF1ADFF9 HTTP 1.1" 200 1318 "http://act.do?arcfor.org (num_02) "GET /category_id=SUF_26&JSESSIONID=SDISL9F1ADFF9 HTTP 1.1" 100 [] "GET /category_id=SUF_26&JSESSIONID=SDISL9F1ADFF9 HTTP 1.1" [] "GET /category_id=SUF_26&JSESSIONID=SUF_26&JSESSIONID=SUF_26&JSESSIONID=SUF_26&JSESSIONID=SUF_26&JSESSIONID=SUF_26&JSESSIONID=SUF_26&JSESSIONID=SUF_26&JSESSIONID=SUF_26&JSESSIONID=SUF_26&JSESSIONID=SUF_26&JSESSIONID=SUF_26&JSESSIONID=SUF_26&JSESSI om/category.screen?categ noing /oldlink?item_



"But what about #machinelearning?"



Machine Learning

Our Approach

- Correlate data sources across 50+ metrics for individuals, product types, regions
- Identify patterns & behaviours with classification models

Screen?product id=FL-DSH-01&JSE

- Train classification model
- Detect Rogue Traders!



ML Classification Models



Adaptive Limit Anomaly Detection





Use ML Alongside Prescriptive Rules



Higher_Risk_Trading 🛇	
High	1
Medium	1
Low	1
Low	1
Medium	1
Medium	١

iunics App Search & Re-	v pring v						Administrator v Messages v	Settings - Activity - Help	
arch Pirot Reports	Alerts	Deshboards						Search & Reportin	
New Search								Save As ~ Close	
ndex-oldena								Last 34 hours ~ Q	
122,634 events (4/3/14 1:00:00	000 PM to -	4/4/14 1.45:55.000	PM)				Job V II II JA	A & Worbone Mode ~	
ris (122,634) Statisti	a \ 1	Veualization							
nat Timeline - Zoom	0u + 2)		a Centera					1 hour per colum	
								4	
			6.00 PM Thu Apr 3 2014		12:00 Abd Fit Age 4	6:00-AM		12:01 PM	
		Raw - Forma	t.v SD Per Page v				Chur 1 2 3 4 5	6 7 8 9 Net)	
ndes a Al P	-	f Event							
						IONID-SDISLBFF4ADFF7 HTTP 1.1" 200 929 "http:/		n?category_id=0CSPLANPROTO	
d Fields					- Hereiten er	o) Version/5.0.2 Mobile/80600 Safari/6503.18.5 88JSESSIONID+S07SL8FF3AOFF7 HTTP 1.1* 200 362		hart Long Address of Countries	
100+					ile/WEDP-2.1 Configuration/CLDC-1.1 Ver		and the second statement of the second second second	- 01 1 100- 000 101 01 101 101 101 0-1	
hour 34	1					<pre>groduct_id=8A-WDPHIE-JUICEPHCKPLUSAJSESSIDNID= d 3.1: de=de: GT=P7510 Build/WEU07) ApplewebKI</pre>			
mday 2 minute 60	1	> 10.2.1.34 131.178.233.243 (047Apr/2014 13145)54(30014) "GET /product_screen/product_id=AC-SIERMA-HOTSPOIAGAJESSIONED-5078,5473A0473 HTP 1.1* 503 967 "http://shap.spluektel.com/product_screen/product_id=AC-SIERMA-HOTSPOIAGAJESSIONED-5078,5473A0473 HTP 1.1* 503 967 "http://shap.spluektel.com/product_screen/product_screen/product_id=AC-SIERMA-HOTSPOIAGAJESSIONED-5078,5473A0473 HTP 1.1* 503 967 "http://shap.spluektel.com/product_screen/product_id=AC-SIERMA-HOTSPOIAGAJESSIONED-5078,5473A0473 HTP 1.1* 503 967 "http://shap.spluektel.com/product_screen/product_id=AC-SIERMA-HOTSPOIAGAJESSIONED-5078,5473A0473 HTP 1.1* 503 967 "http://shap.spluektel.com/product_screen/product							
month 1 second 60 wday 2 year 1 zone 1		> 2014-04-04 13:45:164, fuert (Event-OpdateBillingProducte, timestamp-13757542, properties-LARGOrrelationD=Ma, #OMestageD=201657-05.50070877754107182772, order3ype=MemActivation, quatehrierity=MOBMA, conversat add=58=-70005MACMEXEDD13004050.ccEWB12MM812059, creatis=Ma, _MEMp25=pa.es.pwericespin=timeTailve=h, serviceSame=SpaceBillingProvisioning, es=AXX2755559984, accountumber=V0005580, methodus enformancespin=testimeSizesBillingProvides, endownees-7551578, gatewater-1575157, https://doi.org/10.1017/j.methodus=3201505175127512053093, accountumber=V0005580, methodus enformancespin=testimeSizesBillingProvides, endownees-7551578, gatewater-15751578, gatewater-1505580, restricture "V0007111", martexize=Ph, martexize=Ph, martexize=75097, subdillAppent-1, phoneSuber-1575157, phoneSuber-1555157, planType=PostFaid, glanPrice=8, 99, glantame "200 Nitrure Fails", salarexize=7500 Nitrures", network(1000518270, plantame=7508107, gatewater-1500518270, plantame=7508107, glantame=7508107, glantame=75							
ype 7		> (04/Apr/205	4 13:45:53:974813] pro-mysgl-	.splunktel.com transaction_sp	eed+164 cpu_util+66 mem_util+52 query+*	SELECT * FROM sessions WHERE session_id+'71356	679153.**		
1	1	> [04/Apr/205	4 13:45:53:373442] src-sysgl-	.splunktel.com transaction_sp	eed+10 cpu_stil+55 mem_stil+40 query+*	SELECT * FROM customers WHERE customer_id=1945	561*		
i	1	> (04/apr/201	4 13145(531979181) src-mysel-	.splumitel.com transaction_sp	eed+162 cpu_util+56 mem_util+45 query+*	SELECT product_id, sky, price, FROM products	WERE product_1d+1580*		
oune 5	1	> [04/04/14 1]	3:45:53:507] 000000be Query	E com.ibm.icm.de.portabl	Le.query.Query openQueryCursor() Param	Marker 1: Type - Long			
od 2 t 100+						SELECT price FROM products WHERE product_id+18			
ime 100+						SELECT * FROM customers WHERE customer_id=1924			
te 7	1					<pre>/WanageSearchCollections.jsp]: Initialization</pre>			
rtjpe 7 Ljserver 1	1					ONID-SD75L4FFEADFF3 HTTP 1.1" 200 806 "WERp1// like Geckup Version/4.0.4 Mobile/78067 Safari		addtocart&iten3d=EST-138pr	
nt 40	1	> [04/apr/205	4 13145(51)974283] src-mysql-	.splumktel.com transaction_sp	eed+120 cpu_util+60 mem_util+67 query+'	SELECT * FROM sessions WHERE session_id='84475	997043**		
endpos 16 dartpos 11	1	> (04/Apr/201	4 13:45:51:972850) src=mysql-	.splumktel.com transaction_sp	eed=109 cpu_util=23 mem_util=55 query="	SELECT * FROM sessions WHERE session_id='94751	198671 ' "		
1	1					d=BT-CK-JABRA-FREENKYBJSESSIONID=SORSL4FF3ADFF N=62_WR=11) AppleWebKit/S33.1 (0FTML, like Geo			
sting Fields		> Apr 04 13:4	5:51:079017 ama1 radiusd(2363	:[10 959576 local1.info] DWO	RADOP(13) acct stop for 97783158198sp3	unktel.com 10.149.191.81 from 64.66.0.20 recor	nded GK.		
util 41	1					A, JMSMessage10+10:ESP-PD.840004C7333FC:F45351 InwToLive-1, serviceName-UpdateBillingProvisi			

orobable_cause ≎	isOutlier 🗘			
OutsideHoursTrading	🛕 1			
	✓ 0			
	✓ 0			
	✓ 0			
	🗸 0			
	✓ 0			



The Splunk Value Evolution



Add Us On LinkedIn!



Thank You

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

