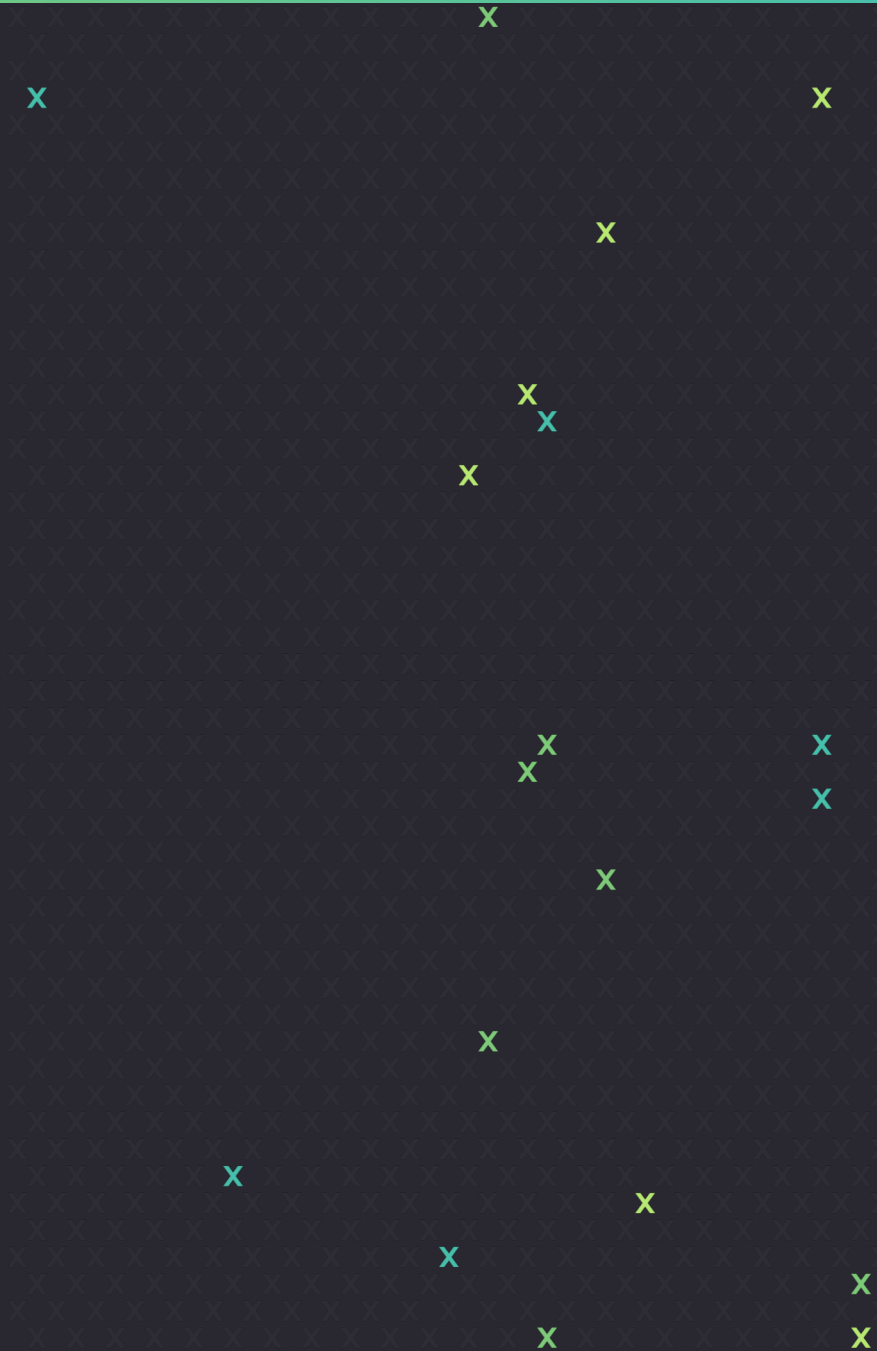




PUT THE MACHINES TO WORK: Security Automation Through Analytics



About Me

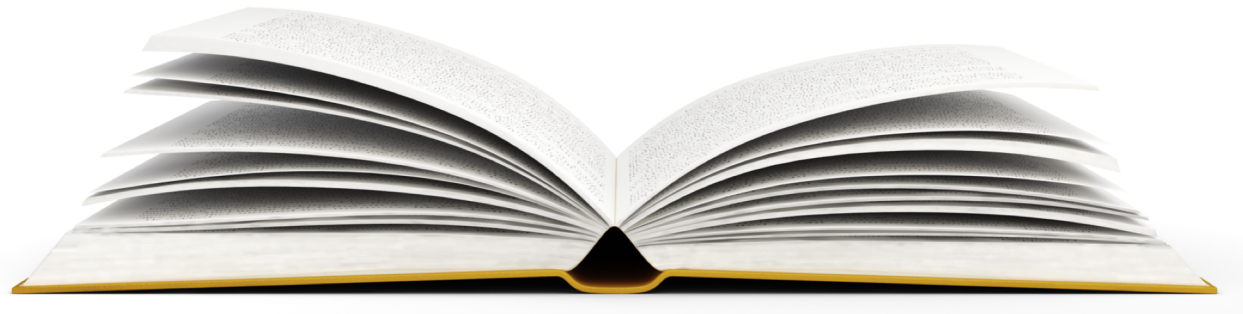
Speaker: Andy Skrei

- VP Worldwide Sales Engineering at Exabeam
- Previously worked as a Lead Security Engineer at eBay developing and deploying technologies for their global SOC
- Prior to eBay, manager at KPMG, helping some of the largest organizations in the world increase security maturity and reduce risk



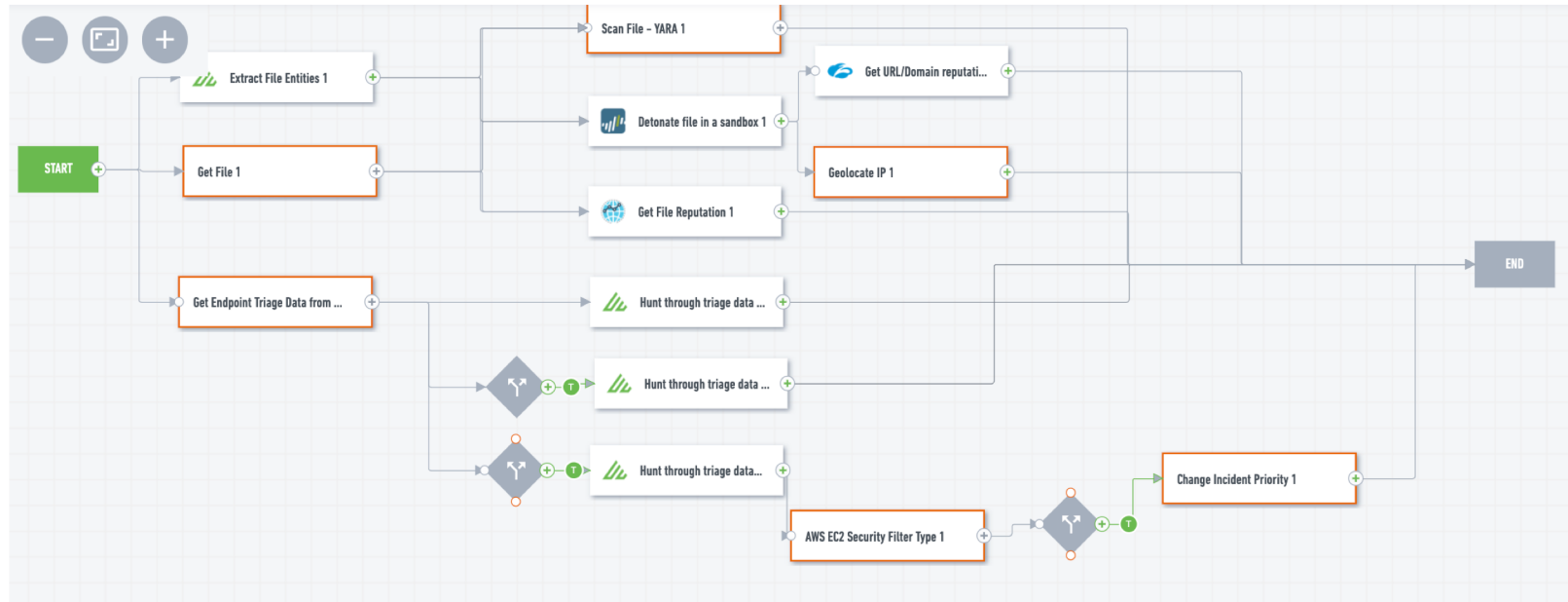
Agenda

- Common Misconceptions
- Level 1 Automation
 - Building a framework
 - Understanding scope
- Level 2 Automation
 - Context
 - Answering expensive questions
- Level 3 Automation
 - SOAR



Common misconceptions

- Ill just throw machines at my problem
- I need end to end automation down to remediation
- My malware playbook only needs to focus on the endpoint









Data Lakes/SIEM

Don't start automation without seeing the full picture

Level 1 Automation: Timelines

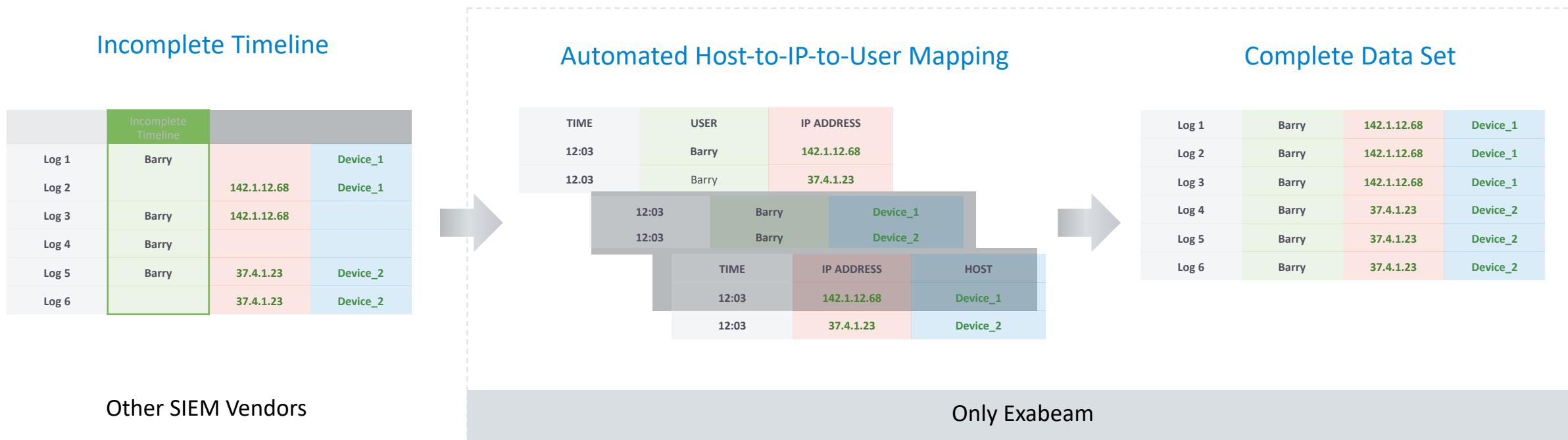
Logs Don't Contain Data Needed to Recreate an Attack
Analysts must manually connect-the-dots, or risk missing parts of an attack

	⚠ Incomplete Timeline		
 Log 1	Barry		Device_1
 Log 2	?	142.1.12.68	Device_1
 Log 3	Barry	142.1.12.68	
 Log 4	Barry		
 Log 5	Barry	37.4.1.23	Device_2
 Log 6	?	37.4.1.23	Device_2

Smart Timelines Automatically Fill in Missing Holes in Log Data

Smart Timelines stitch together log data in real time to fill in the holes, from:

- Millions of logs
- Thousands of users and machines
- IP addresses that change constantly



Intelligence Absent of Context is Irrelevant

Level 2 Automation: Context Enrichment

- BA brings context to log data
 - ▶ Identity
 - ▶ Peer groups
 - ▶ Asset/User tags
 - ▶ Threat Intel
- Machine Learning can create new context
 - ▶ Asset types
 - ▶ Asset Ownership
 - ▶ Account types
 - ▶ Peer groups
 - ▶ DGA
 - ▶ Account associations
 - ▶ Daily activity change

☰ Target credentials for user

CONFIDENCE	EVENTS	VALUES	LAST UPDATE
Excellent - 100%	52	2	a year ago

Enter text to filter



ACCOUNT

COUNT

PCT.

slee

47

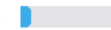
90%



bsalazar

5

10%



First access to this domain

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com which
has been identified as DGA

+10

Level 2 Automation: Answering The Expensive Questions

- Raw events don't tell whole story
 - ▶ Has this user logged in via VPN?
 - ▶ Has the user connected from this IP/Geo?
 - ▶ Has this user connected from this asset before?

```
msg: Login succeeded for bsalazar/kt.com (session:00000000) from 82.117.234.169. | suser: bsalazar | agentSeverity: Unknown |  
exa_adjustedEventTime: May 2nd 2018, 09:44:00.000 | deviceVendor: Juniper | dvc: 192.168.25.240 | dvchost: vpn_srv_1 |  
exa_rawEventTime: May 2nd 2018, 09:44:00.000 | @version: 1 | host: vpn_srv_1 | deviceProduct: Pulse Secure Access |  
exa_parser_name: cef-generic | shost: cc559 | indexTime: Jan 17th 2019, 19:11:25.237 | eventId: 26570628 | src: 82.117.234.169 |  
dtz: US/Central | Vendor: MicroFocus ArcSight | @timestamp: Jan 17th 2019, 19:00:42.155 | port: 56954 | forwarder: 10.14.33.163 |  
data_type: cef-format | event_name: Login Succeeded | time: May 2nd 2018, 09:44:00.000 | _id: AWheuInTjh6Fl5oUDKPN | _type: logs |  
_index: exabeam-2019.01.18 | _score: - |
```


Questions Answered Automatically

- Analytics Provides the Answers
 - ▶ User has never connected from the Ukraine
 - ▶ User has never connected from this IP
 - ▶ User has never connected to the VPN from this device

VPN login from Ukraine			First time activity from country Ukraine	+20
TIME 3:52:00	USER bsalazar	ACCOUNT bsalazar	First activity from country Ukraine for organization	+15
SOURCE IP 82.117.234.169	SOURCE HOST cc559		First activity from ISP VELTON.TELECOM Ltd	+15
COUNTRY Ukraine	ISP VELTON.TELECOM Ltd	VPN ASSIGNED IP 10.77.129.122	First VPN connection from device cc559 for Barbara Salazar	+15
VPN SERVER vpn_srv_1	VPN SERVER IP 10.37.0.124		First VPN connection from device cc559 for organization	+10
VPN VENDOR Juniper VPN	VPN REALM —	OS —	Risk transfer from past sessions	+8
			First connection from source IP 82.117.234.169	+5
			First activity from country Ukraine for group usa	+3

Level 3 Automation: SOAR

- Malware Playbook with Analytics
 - ▶ Where did the malware come from
 - ▶ Remediate access to malicious domains
 - ▶ What did the malware do
 - ▶ Where did the malware spread
 - ▶ Where the credentials compromised



Fredric Weber

[bsalazar, fweber]

Web Developer | Atlanta

TOP PEER GROUP

107

+8 more groups

MANAGER

—

LAST SCORE

237

FILTER	12:20	Web access to dlknknlnkaa.zoomer.cn	First time a user is accessing an internet IP address in this country China	+5
			First access to an internet IP address in this country China for the organization	+5
	13:02	Remote access to srv_246g_stage	Abnormal access to srv_246g_stage for Fredric Weber	+10
			Abnormal access to srv_246g_stage for group CN=Harris Oliver,OU=Users,OU=acetomato,DC=lab,DC=lo	+1
	13:03	Remote access to srv_1020p_dev	Abnormal access to srv_1020p_dev for Fredric Weber	+10
	13:08	Remote access to srv_482k_prod	First access to srv_482k_prod for Fredric Weber	+10
	13:17	Remote access to sea-addc-005	Abnormal access to sea-addc-005 for Fredric Weber	+10
	13:54	Remote access to kt_file_116_prod	Abnormal access to kt_file_116_prod for Fredric Weber	+10
	13:57	Remote access to kt_file_118_prod	Abnormal access to kt_file_118_prod for Fredric Weber	+10
	14:13	Remote access to srv_fileapp_3	First access to srv_fileapp_3 for Fredric Weber	+10
	14:20	Remote access to kt-sg200-wp1	Abnormal access to kt-sg200-wp1 for Fredric Weber	+10
	15:46	Palo Alto Networks alert Malware found on host on lt-fweber-888	Security Alert Malware found on host on asset lt-fweber-888 during a VPN session	+40



Thank you

