PUT THE MACHINES TO WORK: Security Automation Through Analytics

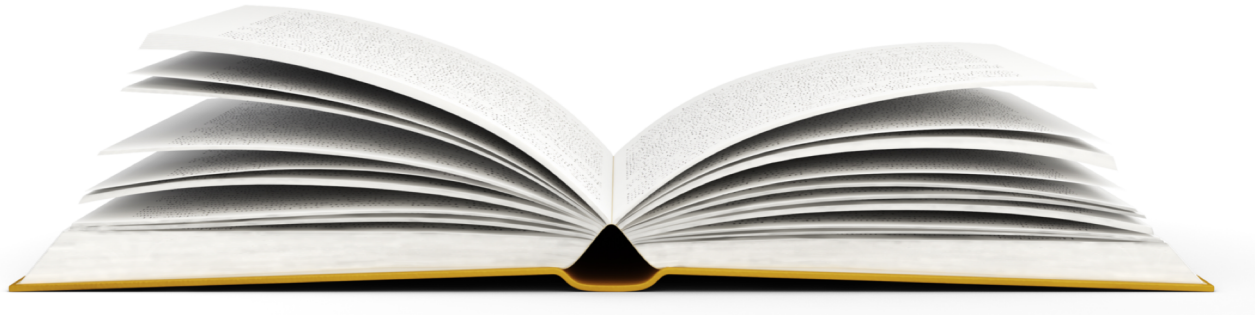
About Me

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 th largest organizations in the world increase security maturity and reduce risk

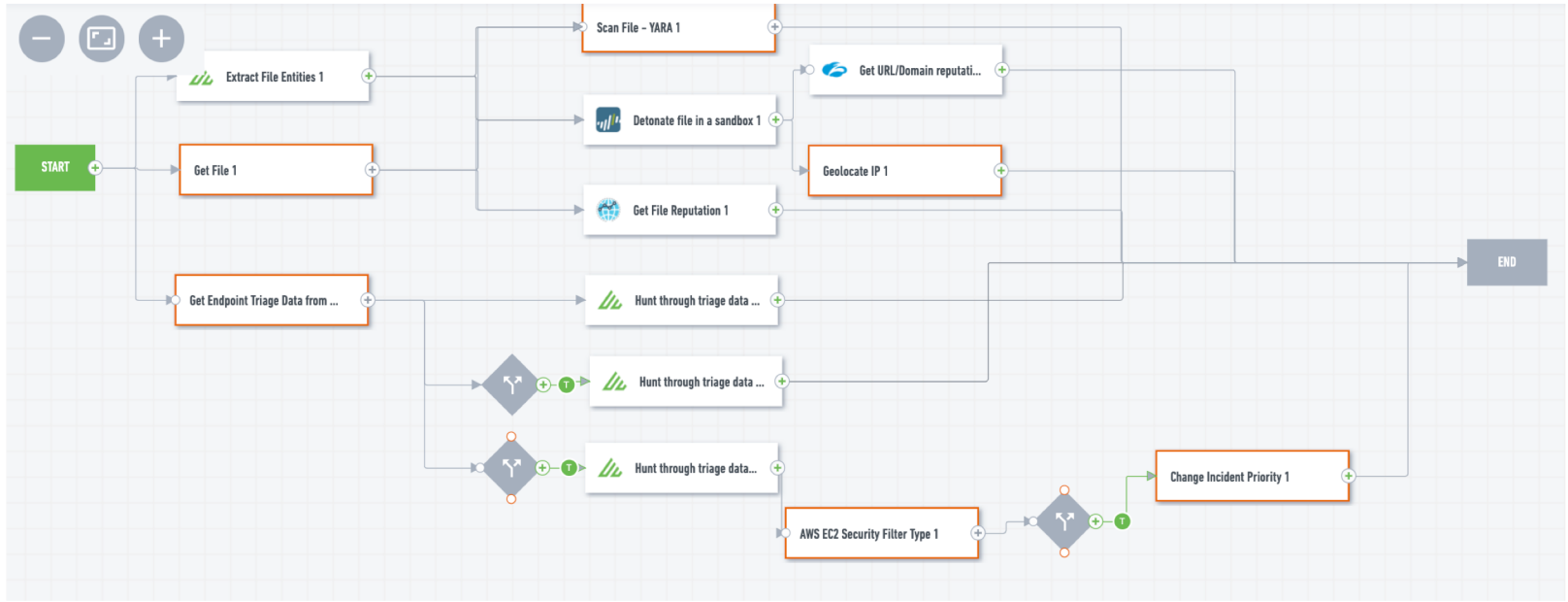
Agenda

- 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

Incomplete Timeline

	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

Other SIEM Vendors

Automated Host-to-IP-to-User Mapping

TIME	USER	IP ADDRESS
12:03	Barry	142.1.12.68
12.03	Barry	37.4.1.23

12:03	Barry	Device_1
12:03	Barry	Device_2

TIME	IP ADDRESS	HOST
12:03	142.1.12.68	Device_1
12:03	37.4.1.23	Device_2

Complete Data Set

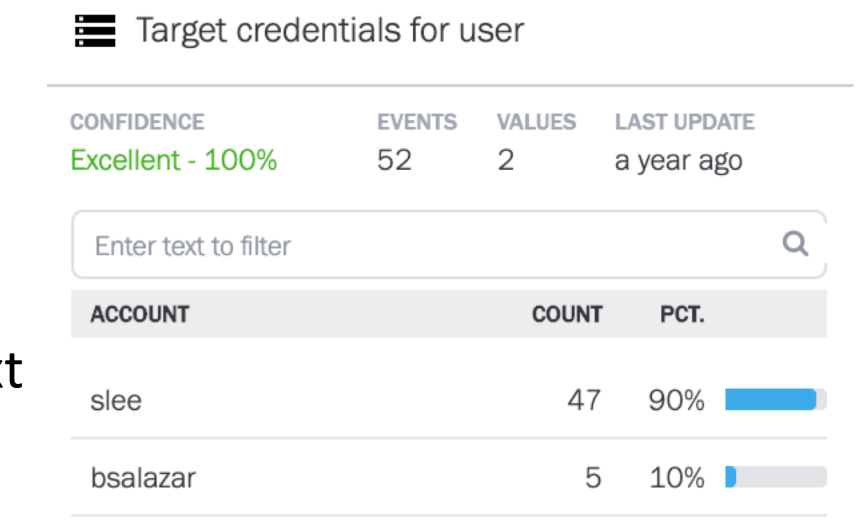
Log 1	Barry	142.1.12.68	Device_1
Log 2	Barry	142.1.12.68	Device_1
Log 3	Barry	142.1.12.68	Device_1
Log 4	Barry	37.4.1.23	Device_2
Log 5	Barry	37.4.1.23	Device_2
Log 6	Barry	37.4.1.23	Device_2

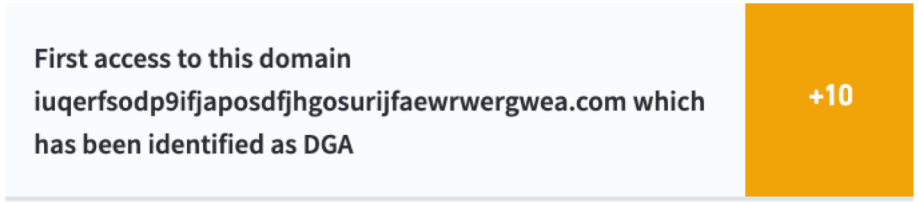
Only Exabeam

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





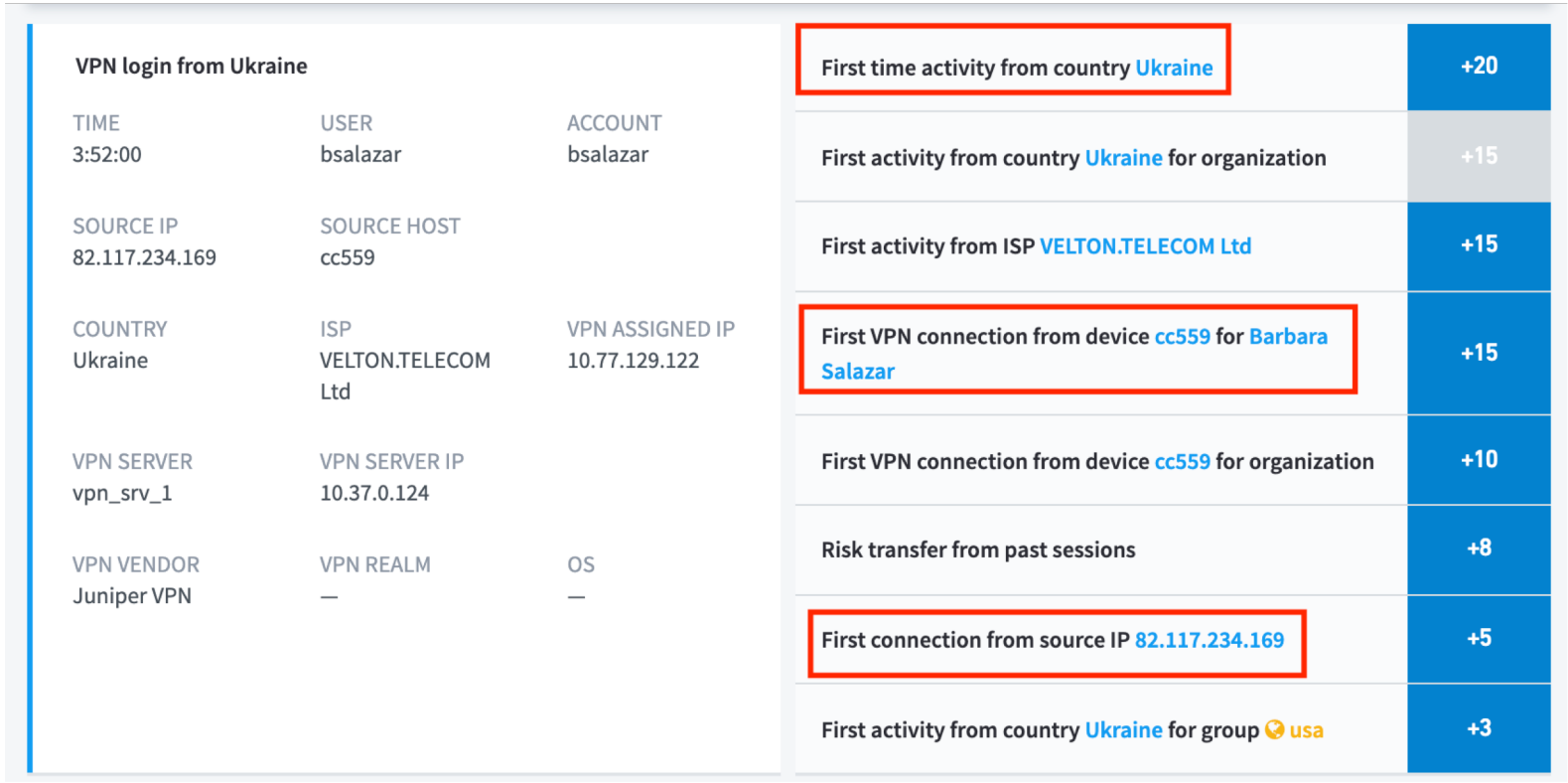
Level 2 Automation: Answering The Expensive Questions

- 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: - |
```

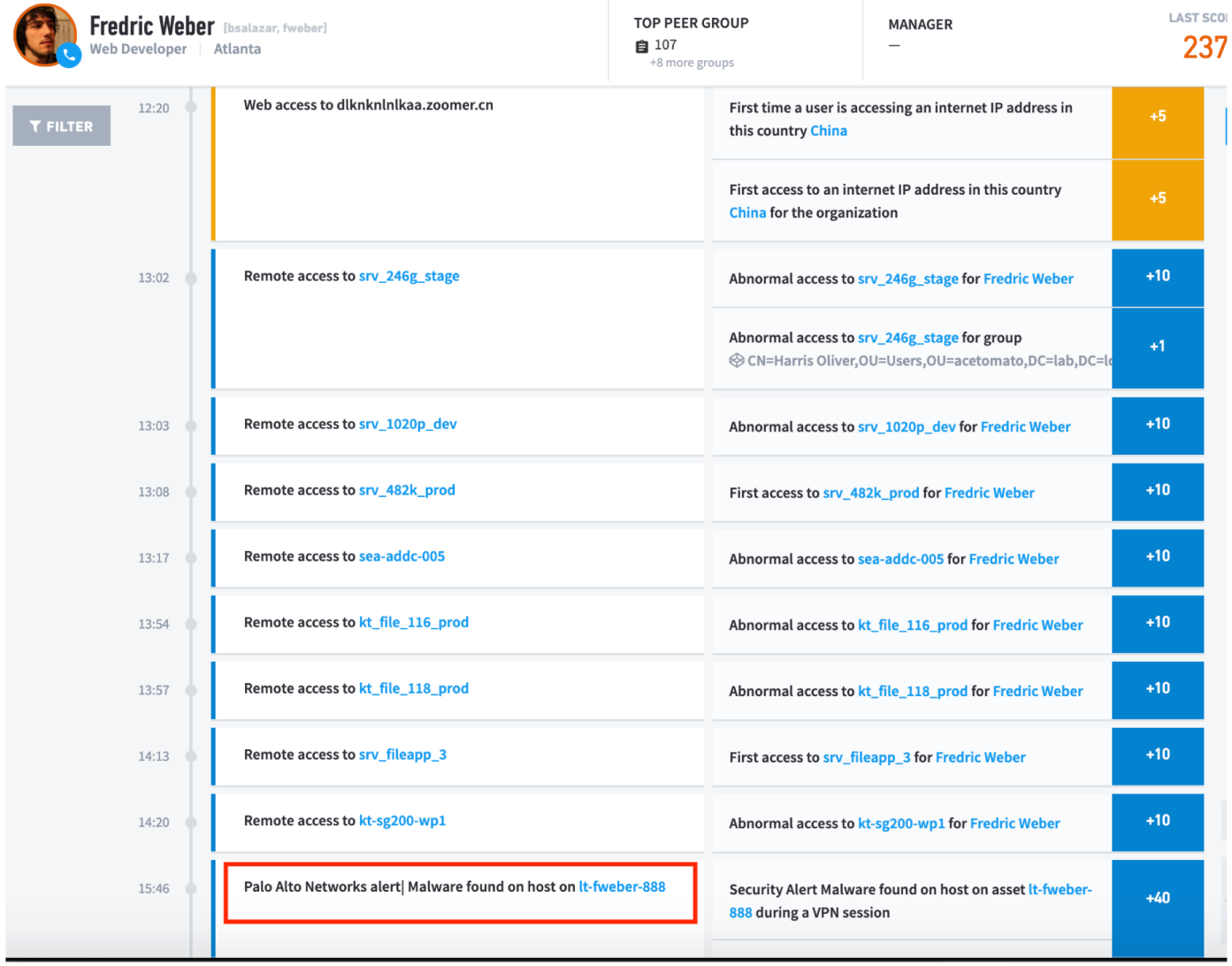
Questions Answered Automatically

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



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



Thank you