



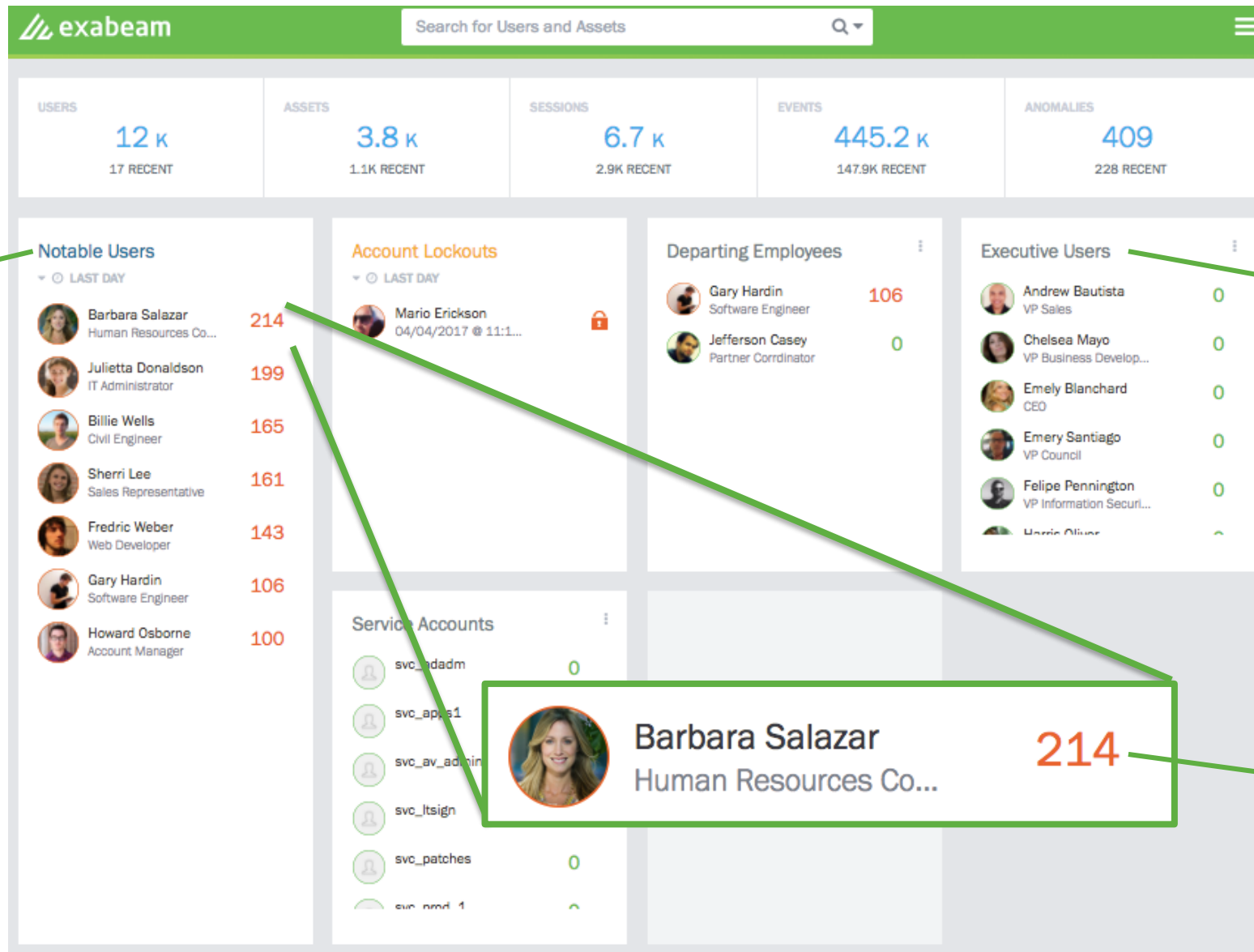
Exabeam AA Slide-based Demo

Somakin Mykola

Confidential



The Advanced Analytics Dashboard



Notable users require investigation - they are exhibiting a high degree of abnormality in their behavior

Customizable watch lists make it easy to keep track of specific types of users or use cases

Anomalous activity results in risk being added to a user's risk score. Higher risk scores mean more unusual behavior.

Quick Investigations of Notable Users

The screenshot displays the Exabeam user profile for Barbara Salazar. The profile includes a contact info button, a 'Contact Info' button, and a 'Watchlist' button. A 'LAST SCORE' badge shows 214. Below the profile is a timeline for Thursday 4/06 at 2:04am to 10:02am, showing a risk score of 214. A line graph shows the risk score trend over time, with a sharp increase on 4/06/17. Below the graph is a 'Risk Reasons' section with a 'Session SCORE 214' badge. The risk reasons list includes: 'Credential switch to a privileged or executive account sa' (+40), '3 x First access to asset' (+21), 'First time user is performing an activity from Ukraine' (+20), and 'Palo Alto NGFW Security Alert on srv_143im_us' (+20).

REASONS	EVENTS	ALERTS	ACCOUNTS	ASSETS	LOCATIONS	SCORE
17	23	1	2	37	2	214

Risk Reasons	Score
Credential switch to a privileged or executive account sa	+40
3 x First access to asset	+21
First time user is performing an activity from Ukraine	+20
Palo Alto NGFW Security Alert on srv_143im_us	+20

User details are displayed to provide analysts context

Risk reasons are written in plain English so analysts can quickly understand what happened

Risk trends help quickly assess when an incident began and ended

Rapid Incident Investigation with Pre-built Timelines

The screenshot displays the Exabeam interface for a user session. At the top, the user profile for Barbara Salazar is shown, including her title (Human Resources Coordinator), division (HR), manager (Tu Petersen), and last score (214). The session summary indicates it started on Thursday 4/06 at 2:04am and ended at 10:02am, with a total score of 214. Below the summary, a table lists various events in chronological order, each with a risk score assigned to it.

REASONS	EVENTS	ALERTS	ACCOUNTS	ASSETS	LOCATIONS	SCORE
17	23	1	2	37	2	214

Time	Event	Risk Score
2:04AM	VPN login from Ukraine	+20
	First time user is performing an activity from Ukraine	+20
	First activity from ISP Vega Telecom Group	+15
	First VPN connection from device cc559 for Barbara Salazar	+15
	Abnormal session start time Thursday 2:04am	+10
	First VPN connection from device cc559 for organization	+10
	First connection from source IP 31.28.161.23	+5
	Risk transfer from past sessions	+5
2:05AM	7 x Remote access	
2:13AM	Remote access to src_k4398_dev	+7
	First access to src_k4398_dev for Barbara Salazar	+7
2:13AM	Remote access to src_n490_dev	+7
	First access to src_n490_dev for Barbara Salazar	+7
2:13AM	Remote access to src_o116_dev	+7
	First access to src_o116_dev for Barbara Salazar	+7
2:14AM	Remote access to src_o118_dev	+3
	Abnormal access to src_o118_dev for Barbara Salazar	+3
2:14AM	Remote logon to colo-sysdb-wp1	+15
	First remote logon to colo-sysdb-wp1 for Barbara Salazar	+15
2:15AM	Account switch to sa on colo-sysdb-wp1	+40
	Credential switch to a privileged or executive account sa	+40


All user activity in an incident (both normal and abnormal) is listed in chronological order

Anomalous behavior is called out and assigned a risk score

Easy Access to Normal Behavior Puts Anomalies into Perspective

exabeam

Q
☰



Barbara Salazar
[bsalazar, sa]

TITLE
Human Resources Coordinator

DIVISION
HR 👤 21

MANAGER
Tu Petersen

☆ **Session Started on Thursday 4/06 at 2:04am – 10:02am**

REASONS 17	EVENTS 23	ALERTS 1	ACCOUNTS 2	ASSETS 37	LOCATIONS 2	SCORE 214
---------------	--------------	-------------	---------------	--------------	----------------	--

0 Comments
vpn
Exabeam Logs
Export Events
Accept Session

<p>2:04AM</p>	<p>VPN login from Ukraine</p>	<ul style="list-style-type: none"> First time user is performing an activity from Ukraine +20 First activity from ISP Vega Telecom Group +15 First VPN connection from device cc559 for Barbara Salazar +15 Abnormal session start time Thursday 2:04am +10 First VPN connection from device cc559 for organization [redacted] +10 First connection from source IP 31.28.161.23 +5 Risk transfer from past sessions +5
2:05AM	7 x Remote access	
2:13AM	Remote access to src_k4398_dev	First access to src_k4398_dev for Barbara Salazar +7
2:13AM	Remote access to src_n490_dev	First access to src_n490_dev for Barbara Salazar +7
2:13AM	Remote access to src_o116_dev	First access to src_o116_dev for Barbara Salazar +7
2:14AM	Remote access to src_o118_dev	Abnormal access to src_o118_dev for Barbara Salazar +3
2:14AM	Remote logon to colo-sysdb-wp1	First remote logon to colo-sysdb-wp1 for Barbara Salazar +15
2:15AM	Account switch to sa on colo-sysdb-wp1	Credential switch to a privileged or executive account sa +40

📍 **Countries for user activity**


Countries from which users have performed some activity. This is based on the source address in vpn login/application login/file access events.

Model as of 4/06/17

CONFIDENCE
Good - 97%

EVENTS
336

VALUES
1



COUNTRY	COUNT	PCT.
🇺🇦 Ukraine ⚠️	336	100%
🇺🇸 United States	336	100%

THRESHOLD

Close



Determine Asset Usage and De Facto Owners via Asset Modeling

exabeam Search for Users and Assets

Barbara Salazar [bsalazar, sa] TITLE Human Resources Coordinator DIVISION HR 21 MANAGER Tu Petersen LAST SCORE 214

Session Started on Thursday 4/06 at 2:04am – 10:02am

REASONS 17 EVENTS 23 ALERTS 1 ACCOUNTS 2 ASSETS 37 LOCATIONS 2 SCORE 214

0 Comments vpn Exabeam Logs Export Events Accept Session

2:04AM VPN login from Ukraine

- First time user is performing an activity from Ukraine +20
- First activity from ISP Vega Telecom Group +15
- First VPN connection from device cc559 for Barbara Salazar +15
- Abnormal session start time Thursday 2:04am +10
- First VPN connection from device cc559 for organization +10
- First connection from source IP 31.28.161.23 +5
- Risk transfer from past sessions +5

2:05AM 7 x Remote access

2:13AM Remote access to src_k4398_dev

2:13AM Remote access to src_n490_dev

2:13AM Remote access to src_o116_dev

2:14AM Remote access to src_o118_dev

2:14AM Remote logon to colo-sysdb-wp1

2:15AM Account switch to sa on colo-sysdb-wp1

VPN endpoints

Models the computers that VPN into the organization

Model as of 4/06/17		Current Model	
CONFIDENCE	EVENTS	VALUES	
Good - 97%	1,151	2	

Enter text to filter

ENDPOINT	COUNT	PCT.
cc559 ⚠		
lt-bsalazar-888	751	65%
wks-b201-731	400	35%

Close



Incident Timelines include Lateral Movement



This symbol indicates a change in credentials, and activity performed using those credentials

2:15AM	Account switch to sa on colo-sysdb-wp1	Credential switch to a privileged or executive account sa +40
		First switch to target account sa for Barbara Salazar +15
4:20AM	Remote logon to srv_sql05	
4:20AM	Login to database service mssql	First access to database mssql for peer group HR +10
		First access to database mssql for user +10
4:22AM	2 x Database query	
4:28AM	Palo Alto NGFW alert Large outbound traffic volume	Palo Alto NGFW Security Alert on srv_143im_us +20
5:22AM	4 x Remote access	

Behavioral Modeling and Peer Grouping Yield Accurate Detection Results

Email received from: [effacaciouscrbays.xyz](#)

Domains per group

Email domains groups send or receive from

Model as of 4/06/17	Current Model
CONFIDENCE Good - 92%	EVENTS 1,351,151
	VALUES 6

Enter text to filter

EXTERNAL DOMAIN	COUNT	PCT.
ktenergy.com	763,112	56%
wellsfargo.com	430,983	32%
salesforce.com	94,822	7%
linkedin.com	53,140	4%
gmail.com	9,093	< 1%
effacaciouscrbays.xyz ⚠	1	< 1%

Close

Abnormal email to/from [effacaciouscrbays.xyz](#) for the organization +10

First email to/from [effacaciouscrbays.xyz](#) +10

Abnormal email domain [effacaciouscrbays.xyz](#) for group Sales Representative +5

User behavior is compared against a user's baseline **AND** that of their peer group

Threat Hunting Based on User Sessions

Searches are performed via a point-and-click interface. Simply select criteria from the dropdown menus and hit search.

The screenshot shows the Exabeam search interface with several filter sections. The 'Dates' section includes a 'Custom' dropdown and two date pickers with values '01/01/2017 12:00 am' and '04/06/2017 12:00 am'. The 'Activity Types' section is highlighted with an orange box and shows a dropdown menu with 'Select an Activity Type' and 'VPN'. The 'Reasons' section is also highlighted with an orange box and contains a text input field 'Enter rule name' and the text 'Non-Executive user logon to executive a sset'. The 'Geo Locations' section is highlighted with an orange box and contains a text input field 'Enter country name' and the text 'China'. Other sections include 'User Names', 'User Labels', 'Peer Groups', 'Assets', 'Asset Labels', 'Scores', and 'Network Zones'. A blue 'Search' button is located at the bottom right.

Threat Hunting Based on User Sessions

The results show all **sessions** which match the search criteria. Each session has a pre-built incident timeline.

The screenshot displays the Exabeam search interface. At the top, there is a green header with the Exabeam logo and a search bar containing the text "Search for Users and Assets". Below the header, a search filter bar is highlighted with an orange border. It contains the following filters: "Dates: 01/01/2017 12:00 am - 04/06/2017 12:00 am", "Activity Types: VPN", "Reasons: Non-Executive user logon to executive asset", and "Geo Locations: China". A "Save" button is visible to the right of the filters. Below the filters, the search results are displayed. On the left, there is a sidebar with various filters: "User Names (1)", "Assets (10)", "Network Zones (1)", "Peer Groups (1)", "Account Names (1)", and "Event Types (5)". The main content area shows a search result for a session. The session is titled "Session (1 results)" and indicates "We found a total of 1 results for your search". The session details include a profile picture of Rob Koch, his name "Rob Koch", his role "IT Administrator", and the session time "04/05/2017 @ 2:04 am". To the right of the session details, there is a table of statistics: REASONS (3), EVENTS (7), ALERTS (0), ACCOUNTS (1), ASSETS (10), and LOCATIONS (1). The overall SCORE is 75. A "Go To Timeline" link is also present.

REASONS	EVENTS	ALERTS	ACCOUNTS	ASSETS	LOCATIONS	SCORE
3	7	0	1	10	1	75

Threat Hunting Based on User Sessions

The screenshot shows the Exabeam user session interface for Rob Koch. At the top, there is a green header with the Exabeam logo, a search bar for users and assets, and a menu icon. Below the header, the user's profile is displayed, including a profile picture, name (Rob Koch), and various attributes: Title (IT Administrator), Division (IT), Manager (Raelene Thompson), and Last Score (75). The main content area shows a session summary for a session started on Wednesday 4/05 at 2:04am and ended at 4:08am. The summary includes a table of metrics: REASONS (3), EVENTS (7), ALERTS (0), ACCOUNTS (1), ASSETS (10), LOCATIONS (1), and SCORE (75). Below the summary, there are buttons for '0 Comments', 'Exabeam Logs', 'Export Events', and 'Accept Session'. The session events are listed in a table with a timeline on the left. The events include: VPN login from China (2:04AM), 3 x Remote access (2:05AM), Remote logon to us-crm-srv1 (2:48AM), NTLM logon to srv_app9 (3:37AM), and VPN logout (4:08AM). The VPN login event has two associated alerts: 'VPN connection from a known anonymous proxy at 123.254.111.191' (+30) and 'First connection from source IP 123.254.111.191' (+5). The Remote logon event has one associated alert: 'Non-Executive logon to executive asset us-crm-srv1' (+40).

Session Summary:

Metric	Value
REASONS	3
EVENTS	7
ALERTS	0
ACCOUNTS	1
ASSETS	10
LOCATIONS	1
SCORE	75

Session Events:

Time	Event	Alert	Score
2:04AM	VPN login from China	VPN connection from a known anonymous proxy at 123.254.111.191	+30
		First connection from source IP 123.254.111.191	+5
2:05AM	3 x Remote access		
2:48AM	Remote logon to us-crm-srv1	Non-Executive logon to executive asset us-crm-srv1	+40
3:37AM	NTLM logon to srv_app9		
4:08AM	VPN logout		

Operational Efficiency: Alert ID Context

ALERT ID: 1420341

1420341

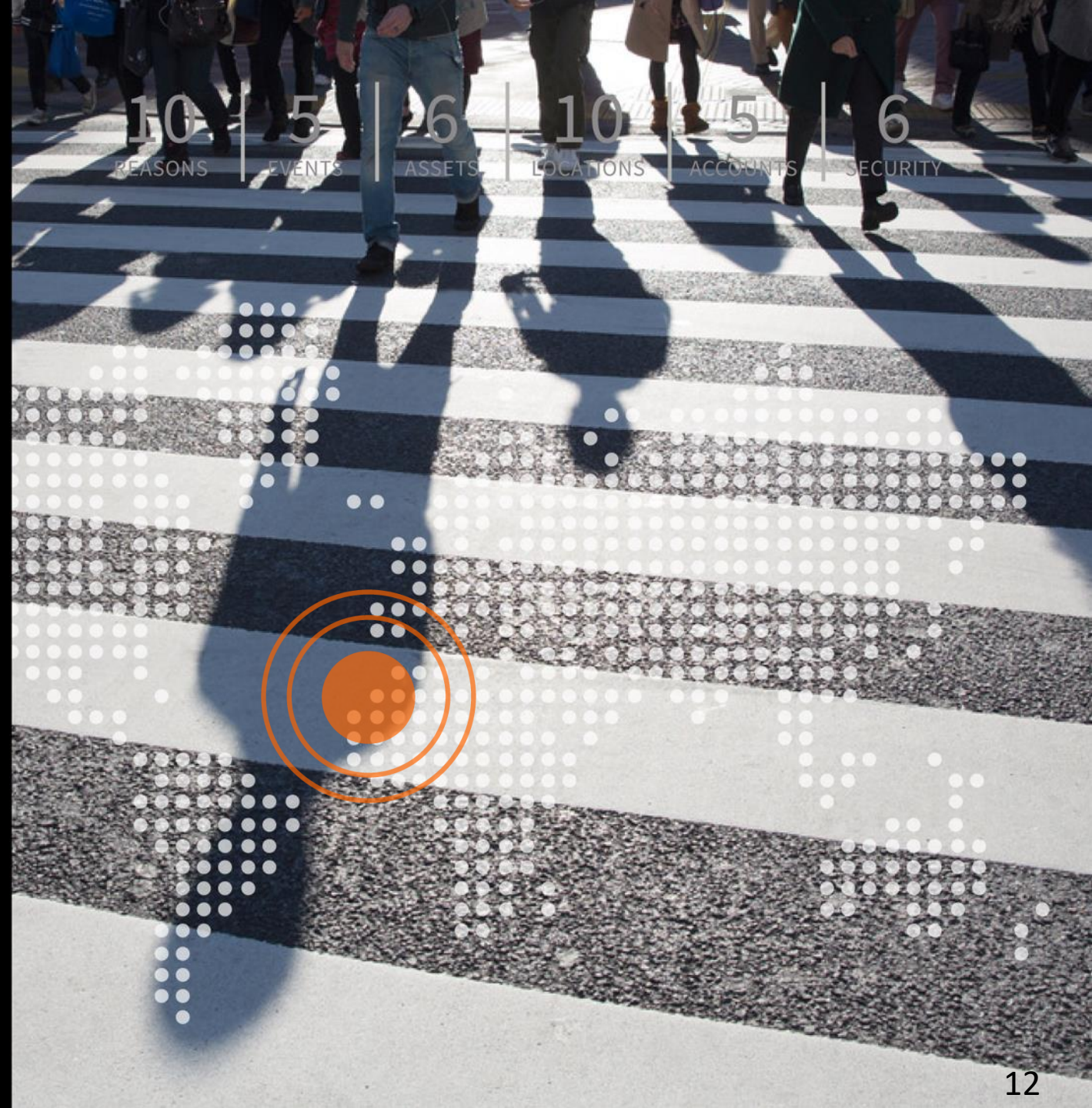
Tied directly to Keesha Hart

Keesha Hart - Operations Director
Friday 9/25, 2015 at 8:37am > 4:10pm
Symantec EPP Salty Malware

Symantec

exabeam

REASONS	EVENTS	ALERTS	ACCOUNTS	ASSETS	LOCATIONS
0	282	0	1	3	0



Thanks

Somakin Mykola