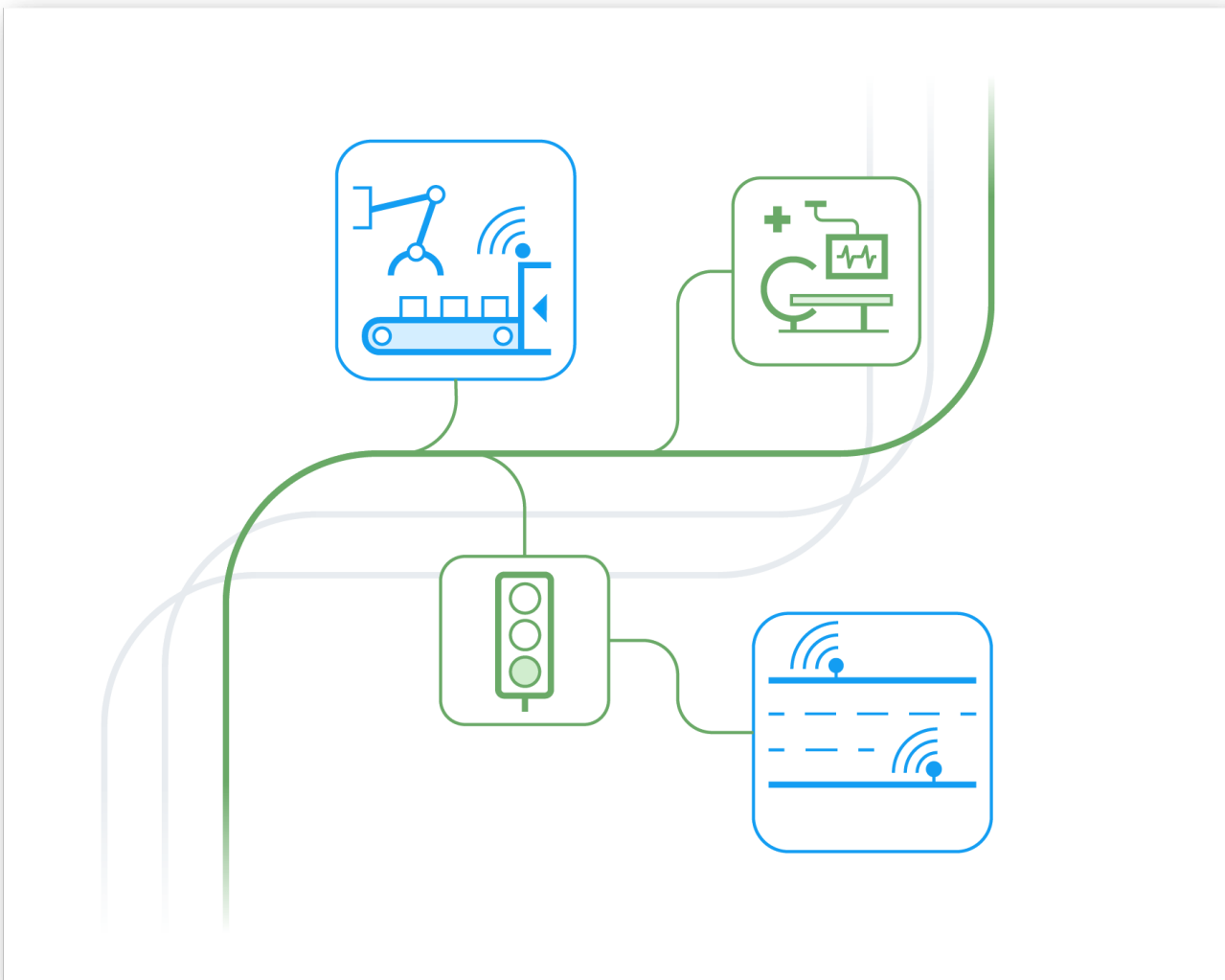


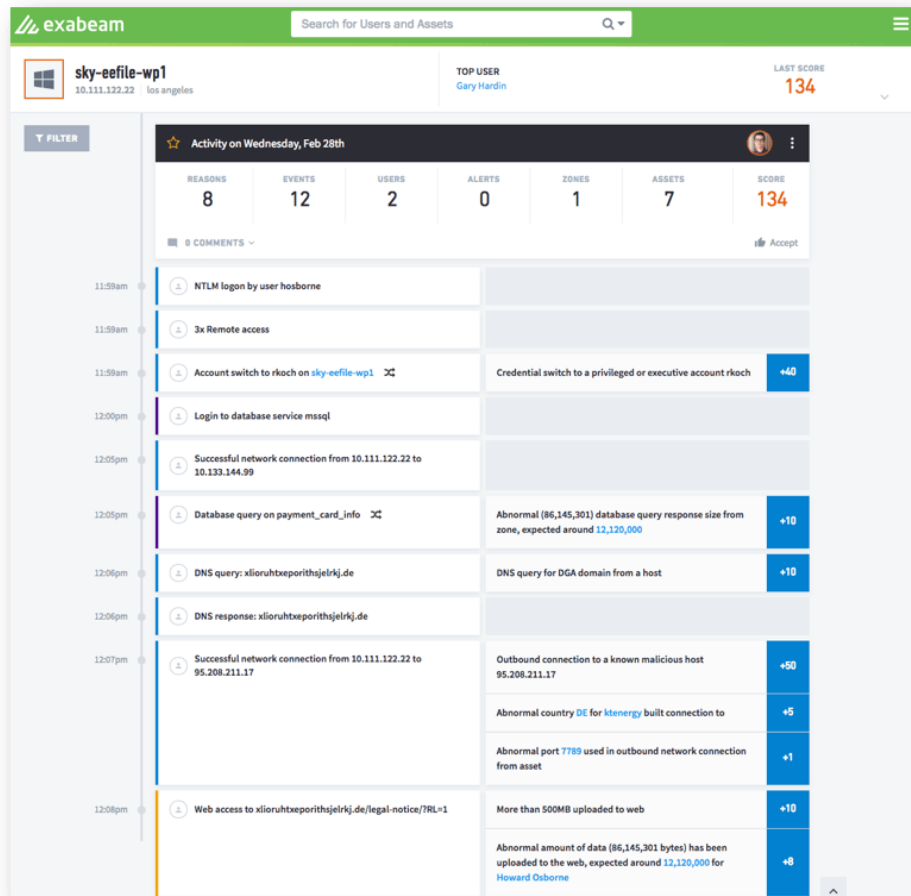
Exabeam Entity Analytics

Behavioral Analytics for Internet-Connected Devices to complete your UEBA solution



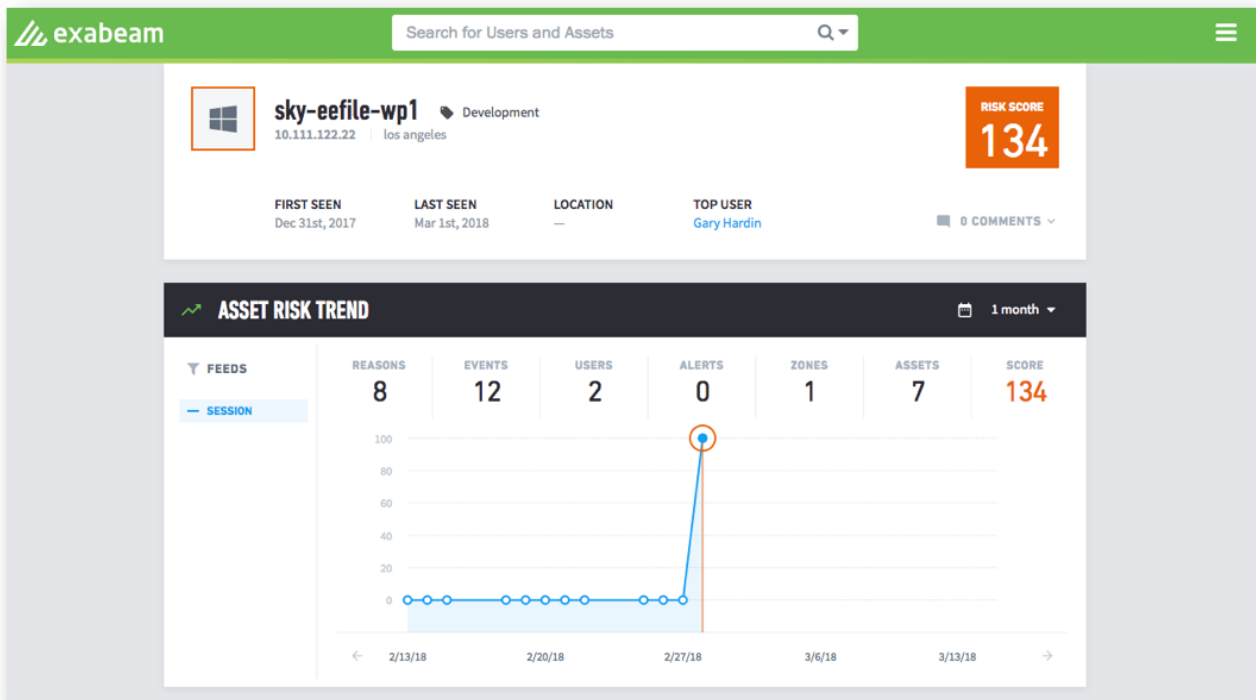
Entity Behavior Analysis

Threats move laterally through a network, leveraging users and machines in their search for high value data. Connected assets like medical equipment, machinery, and power grid infrastructure are an easy target. Assets require the same monitoring as humans. Entity Analytics establishes baseline behavior using communication patterns, ports and protocols, and operating activity — automatically identifying irregular activities indicative of a security incident.



Prebuilt Incident Timelines

Entity Analytics automatically develops timelines of security incidents. Unlike competitive UEBA solutions, Exabeam Smart Timelines track lateral movement without the manual steps. Smart Timelines detail what happened during an incident and identify behavioral context to determine if the activity was normal — reducing the manual efforts of your SOC as they gather evidence for their investigation.



End-to-End Network Visibility

Whether monitoring a LAN or assets from a power grid, data viewed in isolation can appear benign. Exabeam combines and analyzes logs from various sources including VPN, cloud applications, email services, firewalls, NetFlow, and other specific IoT sensors. Machine learning and behavioral modeling that underpin our UEBA solution are then used to detect complex threats that would otherwise go undetected.

The screenshot shows a network monitoring interface for a device named 'sky-eefile-wp1' with IP address '10.111.122.22' located in 'los angeles'. The 'TOP USER' is identified as 'Gary Hardin'. A search bar is present with the text 'Search past IP addresses'. Below it, a table lists IP addresses and their corresponding timestamps. A calendar overlay for April 2018 is visible, highlighting the date 12th.

IP Address	From	To
10.111.122.22	3/1/18 12:08pm	
10.111.122.22	3/1/18 12:07pm	
10.111.122.22	3/1/18 12:06pm	
10.111.122.22	3/1/18 12:06pm	
10.111.122.22	3/1/18 12:05pm	
10.111.122.22	3/1/18 12:05pm	
10.111.122.22	3/1/18 12:00pm	
10.111.122.22	3/1/18 11:59am	
10.111.122.22	3/1/18 11:59am	

Automatic IP Mapping

In most IT environments machines are dynamically assigned IP addresses by DHCP. If an incident occurs, security teams must match which assets correlate with the targeted addresses. This can be a tedious, manual process. Entity Analytics not only performs IP association on current addresses, but also all past DHCP IP addressing over time.

RISK REASONS
+134
SESSION 1
GO TO TIMELINE >

Start: 4:00pm End: 3:59pm
Sort by: Risk Score ▾

- Outbound connection to a known malicious host 95.208.211.17
+50
- Credential switch to a privileged or executive account rkoch
+40
- Abnormal (86,145,301) database query response size from zone, expected around 12,120,000
+10
- DNS query for DGA domain from a host
- More than 500MB uploaded to web
- Abnormal amount of data (86,145,301 bytes) has been uploaded to the web, expected around 12,120,000
- Abnormal country DE for ktenergy built connection to
- Abnormal port 7789 used in outbound network connection from asset

Outbound destination ports per asset
Destination ports of outbound network connections per host

	Model as of 3/01/18	Current Model	
CONFIDENCE			
Good - 92%	6,462	4	
<input type="text" value="Enter text to filter"/>			
DESTINATION PORT	COUNT	PCT.	
80	2,600	40%	<div style="width: 40%; height: 10px; background-color: #007bff;"></div>
443	2,367	37%	<div style="width: 37%; height: 10px; background-color: #007bff;"></div>
118	1,490	23%	<div style="width: 23%; height: 10px; background-color: #007bff;"></div>
7789 ▲	5	< 1%	THRESHOLD

Close

Rule And Signature-Free Detection

Correlation rules and threat signatures create false positives due to their lack of context, and false negatives because they're not able to detect unknown attacks. Maintenance also consumes large blocks of analyst time. Entity Analytics uses behavioral modeling and machine learning to look for abnormal activity — sensing risks and detecting anomalous events — without the tuning, maintenance, and false positives that drain analyst productivity.