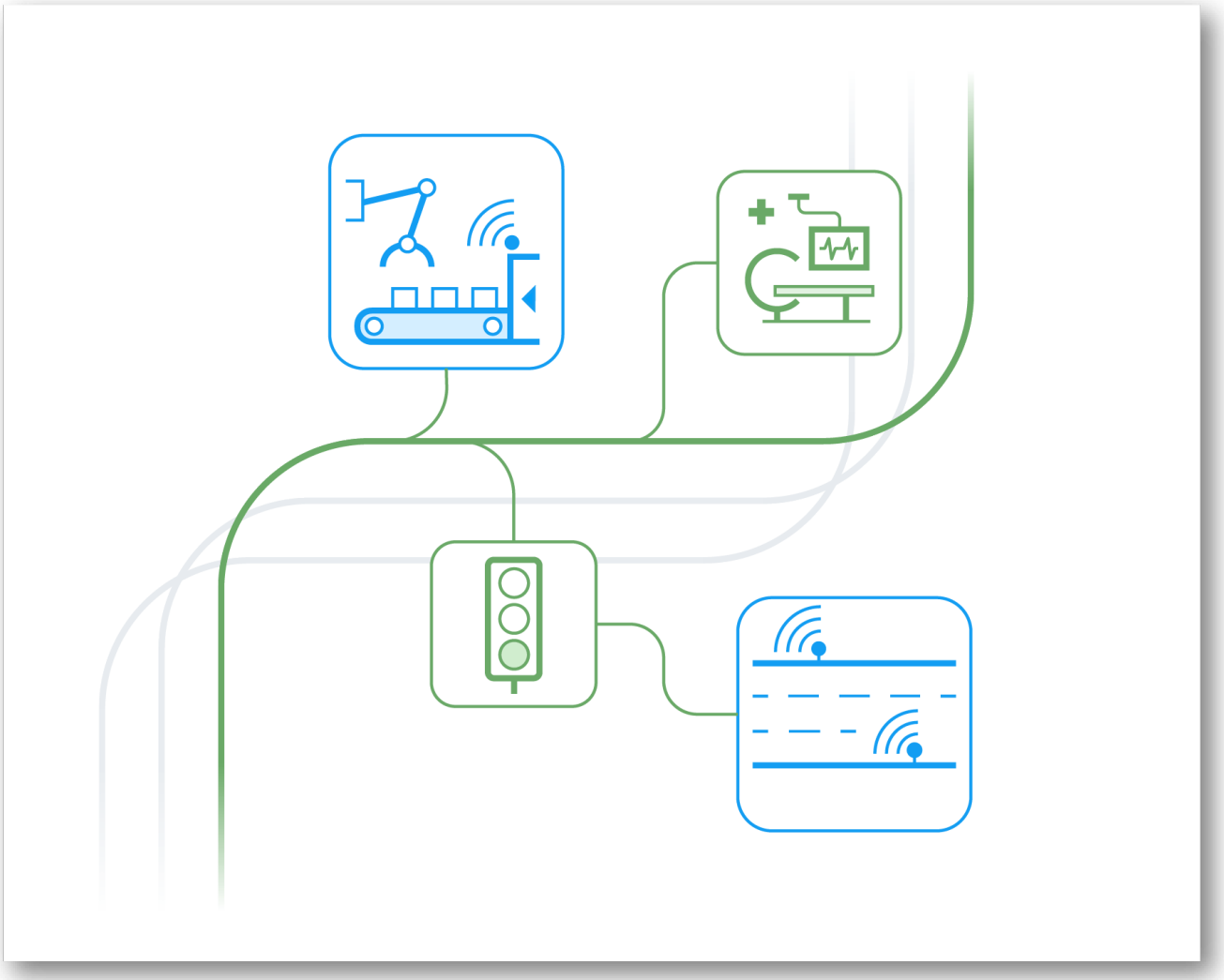
exabeam

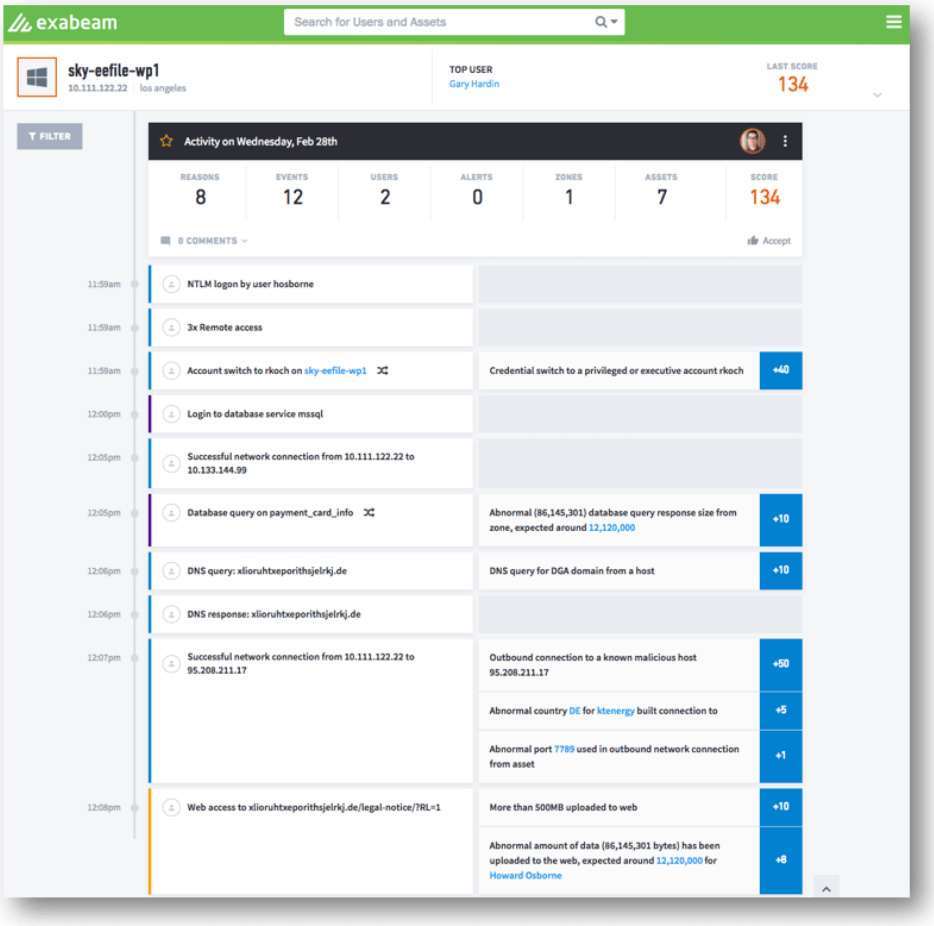
Exabeam Entity Analytics

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



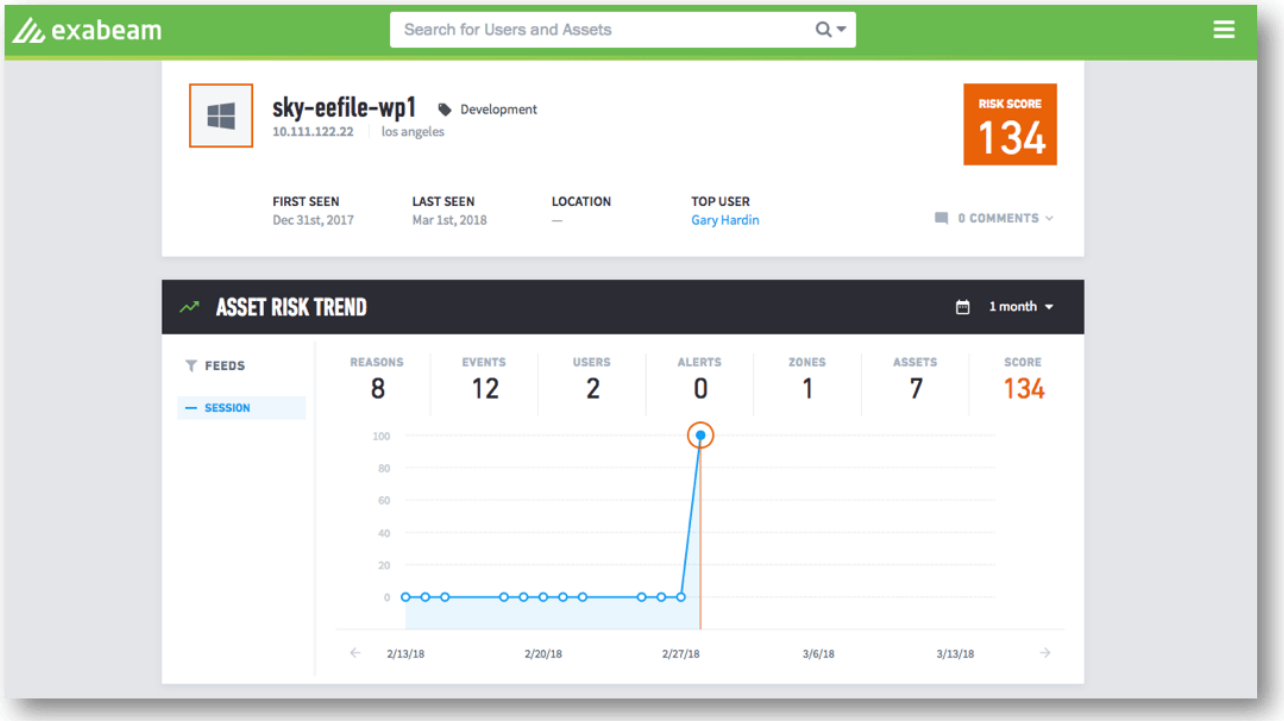
Entity Behavior Analysis

Threats move laterally though 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.



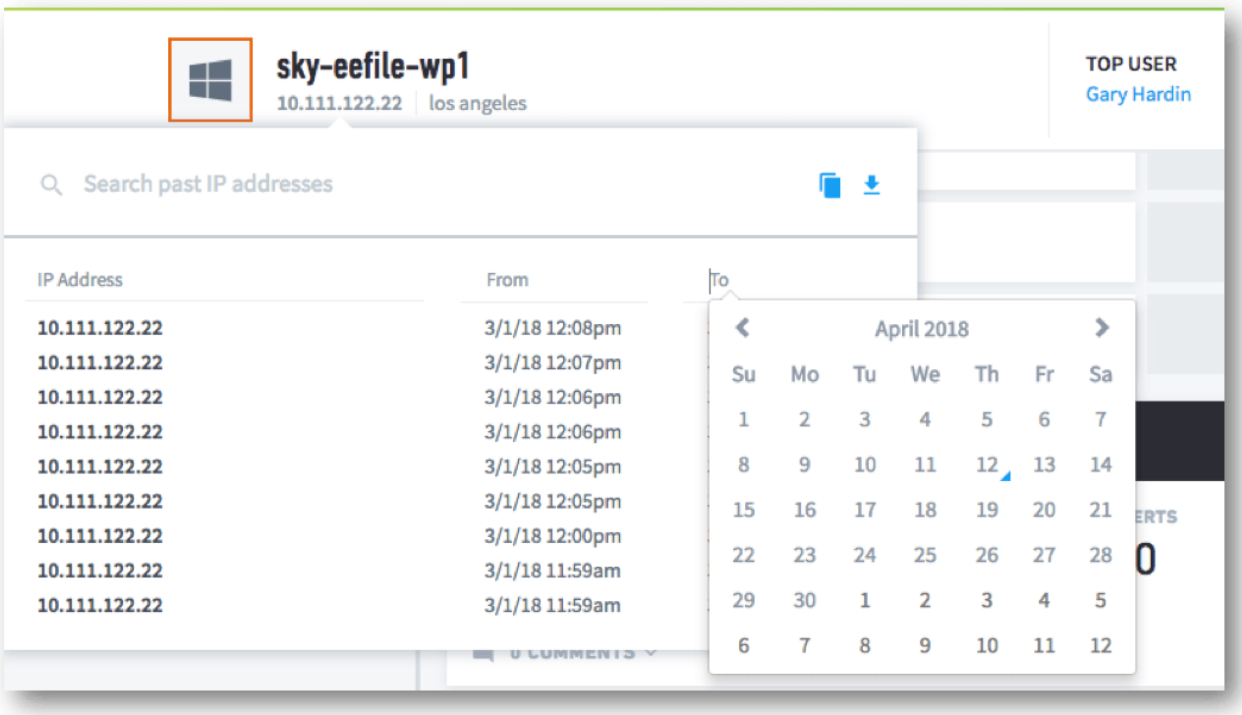
Prebuilt Incident Timelines

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.



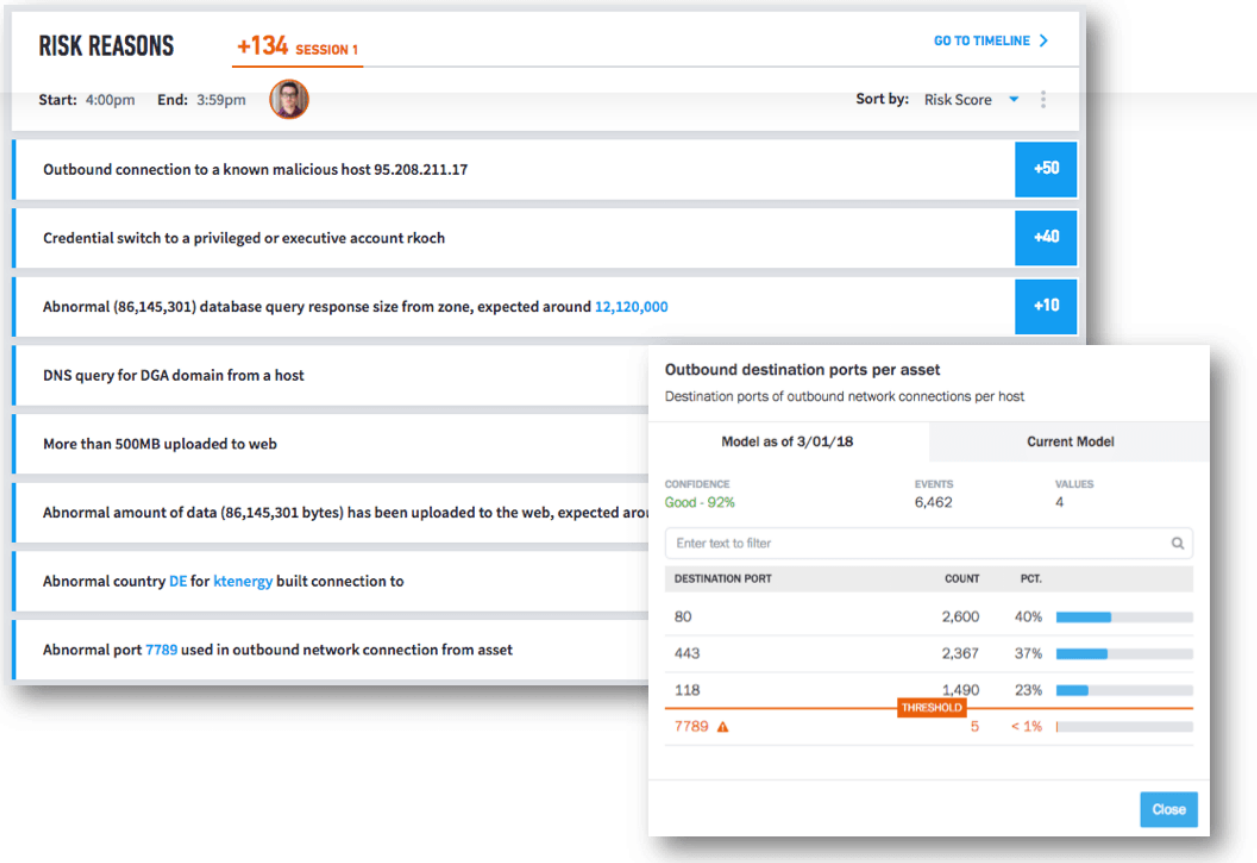
End-to-End Network Visibility

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.



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.



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.