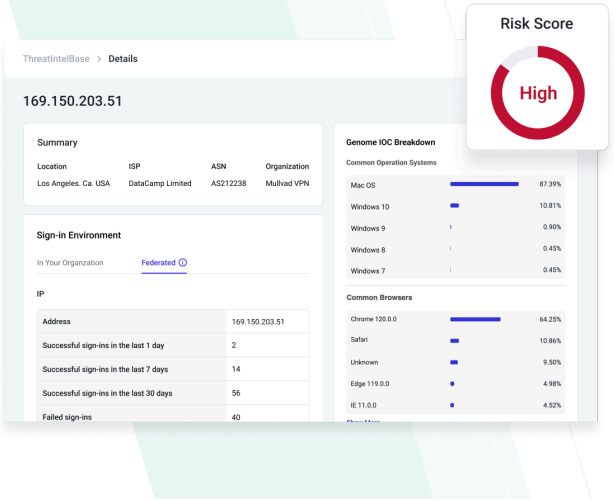
Abnormal

ThreatIntelBase: Behaviorally-Derived Threat Intelligence

Surface cross-customer and cross-platform IP intelligence to streamline SOC processes.

Analysts struggle to leverage threat intelligence across platforms and assess their environments for known threats sourced from intel feeds. They only have visibility into a subset of data related to attacks impacting their cloud email platform. The fractured view makes it challenging to correlate information and only offers a snapshot of an attack, rather than completing the picture.

Abnormal's behavioral AI detection is used to detect zero day attacks within cloud platforms, yielding previously undiscovered threat intelligence. Abnormal already uses this data across products, platforms and customers to improve detection - ThreatIntelBase will allow you to leverage this data too.



Abnormal provides the solution.

Provides insights from behaviorally-derived threat intelligence to allow SOC analysts to investigate suspicious activity across the cloud email platform.

Improves SOC understanding of an account takeover by providing critical indicators of compromise from across their platform and federated across the customer network.

Adds visibility into indicators of compromise associated with user activity across integrated applications, including IOC metadata, associated APTs, common attacks, and behavioral patterns within a customer's environment or the Abnormal federated network.

Enriches the Human Behavior AI Platform with a deeper understanding of each customer's users, vendors, tenants, applications, and IP addresses, surfacing any deviation from the established behavior baselines in Knowledge Bases.

The Abnormal Advantage at a Glance

Faster incident response and investigation with instant, cross-product and cross-platform search for cloud account activity and threats associated with a malicious IP. Use the info to restore compromised accounts, block malicious IPs, and threat hunt related activity.

Superior visibility and context about malicious IOCs, in a single place, with derived insights from Abnormal AI.

Improved efficacy with access to novel, behaviorally-derived threat intelligence to enhance other security products.