DRAWING ON THE POWER OF HUMAN INTUITION TO DEFEND AGAINST CYBER ATTACKS

With Palantir, organizations can improve enterprise-wide situational awareness and obtain a comprehensive understanding of threats facing their networks. Palantir quickly pivots from threat identification to incident response and mitigation, all within the same platform.

Palantir enables customers to harden their defenses against external threats and to rapidly discover, characterize, and respond to attacks and breaches. Palantir integrates all data into a single analytical workspace, revealing patterns, connections, and anomalies among disparate data sources that would otherwise go undetected.

Once a threat has been identified, users can leverage Palantir’s analytic capabilities to understand the extent of the threat and to respond rapidly to reinforce network defense. The Revisioning Database, Palantir’s persistent store, tracks the full history of all data in the enterprise, enabling analysts to collaborate and leverage one another’s work.

Organizations can create customized IP address reputation feeds based on data from several sources to rapidly determine the risk score of IPs hitting the network. Repetitive processes can be automated, and users can configure rule-based persistent alerts for notification when data relevant to their work is ingested.

PALANTIR CYBER

Government and commercial organizations rely heavily on secure information networks, but the traditional patchwork of automated cyber defenses—firewalls, anti-virus software, and intrusion detection systems—fails against adaptive adversaries.

Email, proxy data, and employee badge log data systems were not architected to coexist in the same platform, and few systems are designed to protect the privacy of multiple data formats. The data scale is immense and growing at over a terabyte per day at large institutions. Most platforms can only handle this scale in small chunks, inhibiting trend analysis. Resources are distributed across functional and organizational silos, and organizations lack the command-level perspective necessary to maintain a unified view of security across the enterprise.
PALANTIR IN ACTION
Commercial and government organizations use Palantir to identify and characterize threats as they hit the network:

Financial Institutions: A major financial institution uses Palantir to respond to ongoing distributed denial of service (DDoS) attacks. Palantir integrates, stores, and correlates multiple data sources, including lists of known and malicious IPs, enabling analysts to rapidly identify common properties among DDoS attackers. Shortly after an attack, analysts can share attack vector information through Palantir, including contextual information derived from blog postings and social media sites where attackers publicly take credit for incidents.

Government Agencies: A government organization uses Palantir for command and control. Palantir fuses data from intrusion detection systems, network monitors, and audit logs, creating an integrated picture of the enterprise’s entire infrastructure. Persistent searches alert users to anomalies in monitoring systems or messages about new vulnerabilities from external security organizations. After receiving a tip that a foreign hacker group was using a particular online journal to plan an attack, analysts created intelligence on the group’s peer network and attack pattern using Palantir’s relational, geospatial, and temporal analysis capabilities. Palantir’s powerful security model allowed the agency to share the intelligence with foreign and domestic agencies by automatically redacting sensitive information from reports.

FEATURED CAPABILITIES
• Phoenix: separate signal from noise in petabyte-scale data
• Raptor: federate queries to external data sources without ingesting them into the Palantir repository
• Revisioning Database: explore several hypotheses while maintaining a canonical record and full history of all data and metadata
• Priority Inbox: receive real-time alerts when events and patterns of interest appear
• Collaboration: share messages, objects, and analytical products across the enterprise without jeopardizing the security of the underlying data
• Object Explorer: filter massive amounts of data to discover patterns, trends, and entities of interest
• Dashboard: create customized high-level overviews of all integrated systems
• Access controls: secure each piece of data in the enterprise individually based on roles or classification levels

Multi-perspective analytical applications allow users to rapidly visualize the nature of an attack

Petabyte-scale pattern detection reveals the highest-priority threats facing the network

Dashboards provide a high-level overview of the state of the enterprise