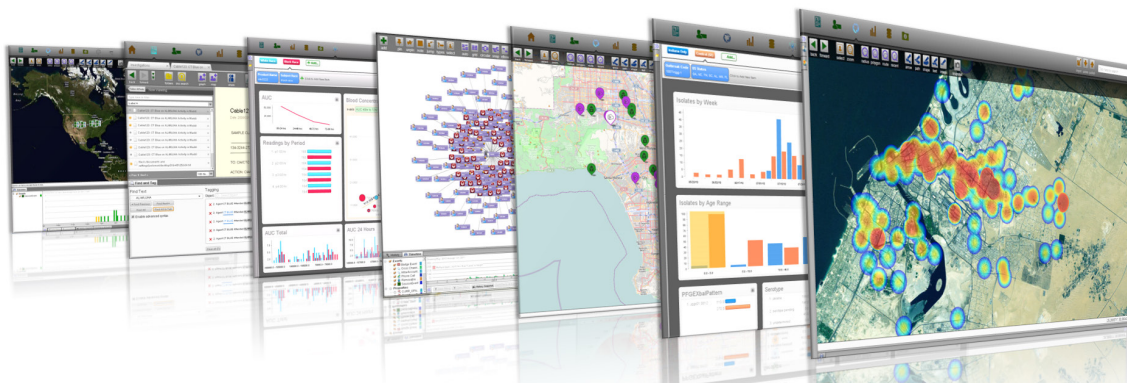


PALANTIR CYBER

An End-to-End Cyber Intelligence Platform for Analysis & Knowledge Management

INTRODUCTION



Traditional perimeter defense solutions fail against sophisticated adversaries who target their victims with complex, adaptive methods. Palantir provides a knowledge management and analysis platform for institutions seeking to understand the nature of cyber threats. Using Palantir, organizations can harden their network defense postures against threats emanating from both external and internal sources.

FUSING INTERNAL AND EXTERNAL CYBER DATA

Palantir integrates data from across the enterprise into a unified environment for rapid analysis, including but not limited to:

- **Structured network logs:** proxy, firewall, IDS, VPN, antivirus, DLP, DNS queries, malware tools, and application access logs
- **Contextual data:** email, print logs, facility access logs, internal chat logs, and HR data
- **Unstructured reporting and third party data:** RSS feeds, vendor reports, government intelligence reports, databases of cyber threat actors, social media streams, IP information, and domain reputation feeds

Out of the box, Palantir can integrate the full spectrum of cyber data. Palantir's pre-built integration pipelines allow our engineers to integrate key data sources just days after the start of a Palantir deployment. Integrated data is immediately available for automated correlation against threat detection algorithms as well as user-driven querying and analysis.

Palantir also ships with a suite of remote cloud-based applications to enhance your enterprise's security posture, enable secure information sharing, and facilitate data reliability. Palantir provides access to collaborative and external cyber resources, including the Palantir Cyber Mesh, Palantir's Cyber Intelligence Feed, and Palantir's Cyber Operations Center.

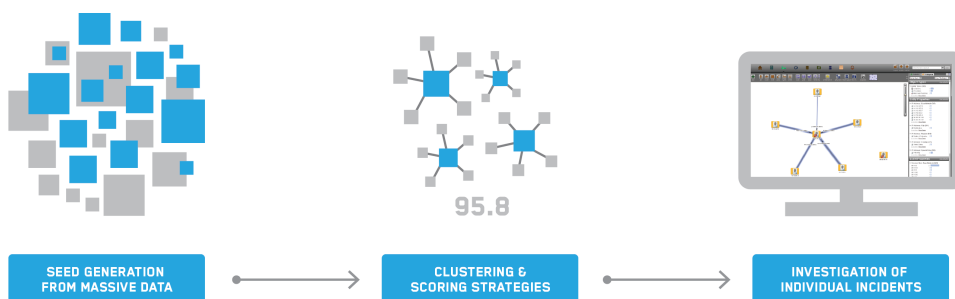
We work with the most sophisticated cyber security organizations in the world, including top-tier financial institutions and international intelligence agencies. Our world-class engineers and cyber security experts enable government and commercial organizations around the globe to prevent and defend against cyber attacks.

THE PALANTIR SOLUTION

At the foundation of Palantir Cyber are three unique capabilities that enable analysts to investigate the origins and features of cyber attacks and devise highly tailored responses. With Palantir Cyber, enterprises move beyond using simple black-box, automated detection systems. Palantir allows organizations to diagnose attacks and take preemptive action against future cyber threats.

ANOMALY DETECTION

Analysts begin cyber threat investigations in Palantir by combing through massive amounts of data to find anomalous occurrences. Palantir Phoenix is a clusterable, distributed data store that enables the integration and sub-second querying of trillions of records at petabyte scale. Architected to scale horizontally across commodity hardware, Phoenix leverages several open source technologies based on Apache's™ Hadoop™ project to manage data at scale and perform advanced analytics, extract files during querying using Apache's Hive™ software to impose a structure on the multiple data formats, and allow the user to focus on a query's semantics rather than efficiency by applying Apache's Pig™ platform.



Organizations use Hercules to conduct automated searches of Phoenix and other data sources, apply customized clustering and scoring strategies, and import events and entities of interest into Palantir Gotham.

Using Palantir's Hercules technology, enterprises build and iterate on strategic algorithms to comb through data archives and detect anomalies by creating clusters that reveal previously unknown entities, events, and connections. The resulting clusters are ranked by relevance and presented to the user along with other visualizations such as risk scores, pie charts, and heat maps. An analyst can triage these clusters and then drill down on a particular anomaly and investigate it further, continually modifying the algorithm as new information emerges.

THE PALANTIR SOLUTION (CONTINUED)




INCIDENT INVESTIGATION

Palantir Cyber provides enterprises with the unified view necessary to correlate incidents of cyber attacks across data sources and monitor cyber threats in real time 24/7/365. Analysts investigate alerts immediately without leaving the workspace, which is crucial in cyber security investigations where incoming information goes stale in hours. Users detect threats by discovering connections between seemingly unrelated events, map hostile activity based on origin, and identify critical vulnerabilities across enterprise systems and networks. Analysts rapidly pivot from threat detection to response and mitigation, streamlining cyber security workflows.

KNOWLEDGE MANAGEMENT

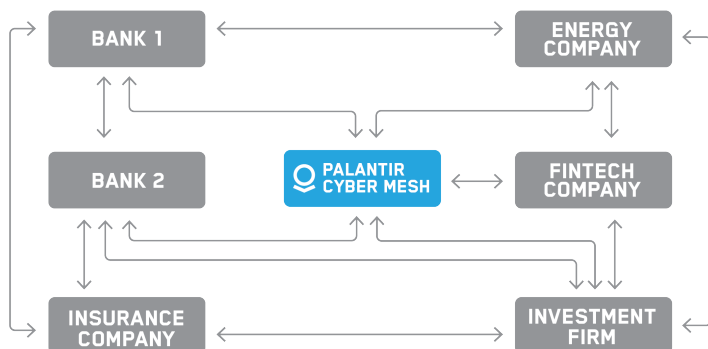
Palantir's knowledge management platform enables institutions to securely store all of their cyber data in one easily searchable environment, in a format accessible to both non-technical and technical analysts. Palantir's central repository allows multiple analysts to work on the same data while engaging in independent lines of inquiry. They can share their discoveries by "publishing" their results, merging their results with others' across the enterprise. This allows for a richly collaborative environment in which each analyst can pursue their own hypotheses and analyses while benefitting from the shared cyber intelligence of others. Analysts can also track how cyber threats change over time and take preemptive action to stop their effects. Enterprises transform from falling victim to cyber threats to conducting proactive counter-intelligence.

All knowledge management activities in Palantir are governed by fine-grained access controls. By "fine-grained," we mean that organizations can secure each and every piece of information in their enterprise individually, rather than applying blanket permissions across entire data sources. This flexibility is unique to Palantir. In this way, organizations can protect privacy and civil liberties while ensuring data security across the enterprise.

DATA	SOURCE	BANK 1'S PERMISSIONS	BANK 2'S PERMISSIONS
 SUSPICIOUS IP ADDRESS	Proxy	NO ACCESS	FULL ACCESS
 MALICIOUS DOMAIN	Proxy	NO ACCESS	FULL ACCESS
 SUSPICIOUS PROXY ALGORITHM	.html repository	READ ACCESS	READ ACCESS

The Palantir Security Model protects data from unauthorized use, allowing organizations to maintain strict access controls. Administrators can assign specific permissions to all data.

PALANTIR'S CYBER RESOURCES



The Palantir Cyber Mesh is a platform for secure information sharing among peers.

THE CYBER MESH

Recognizing that commercial institutions face a shared set of cyber threats, we created **the Cyber Mesh**, a platform for secure information sharing among peers. Drawing on successful models within the defense and intelligence communities, the Cyber Mesh enables secure peer-to-peer sharing between enterprises with automatic redaction of sensitive data. A centrally hosted Palantir instance provides out-of-the-box cyber intelligence feeds, rolled up from suspicious activity patterns, third-party open source and licensed data feeds, and contextual data feeds. By letting organizations leverage the subject matter expertise of Palantir engineers and insights from peer institutions, the Mesh provides immense analytic value over automated black box solutions.

PALANTIR'S CYBER INTELLIGENCE FEED

Palantir's **Cyber Intelligence Feed** is a weighted data feed of Indicators of Compromise (IOCs) drawn from open source and Cyber Mesh participants. Palantir automatically correlates the Feed against customer-owned data sets and presents algorithmic-based alerts for investigation.

PALANTIR'S CYBER OPERATIONS CENTER

Palantir's **Cyber Operations Center** provides on-demand access to our security-cleared engineers who have extensive experience supporting hundreds of deployments. From the Cyber Operations Center, a team of Palantir engineers:

- Monitors system reliability and performance from a secure central location, ensuring critical response coverage at all hours
- Evaluates diagnostic data quickly such as system logs, stack traces, error logs, and overall deployment health

The Cyber Operations Center is a secure facility built to satisfy rigorous federal government security standards such as DCID 6/9 SCIF requirements. Each customer's operations and monitoring environment is kept completely separate from those for other deployments. The facility reflects our experience handling the most sensitive data in the most sensitive operating environments in the world.

ANALYTIC MODULES

We have significant experience deploying Palantir with analytic modules customized for a wide variety of use cases.

INSIDER THREAT DETECTION

Palantir allows enterprises to identify suspicious or abnormal employee behavior using a variety of algorithmic methods that correlate physical presence with logical data access. Palantir's rich time series analytical tools, custom metric capabilities, and configurable dashboards enable organizations to correlate and visualize data both enterprise-wide and for individual investigations. This type of contextual analysis enables decision makers to take informed corrective actions.



Employee attendance correlated with an enterprise's trading activity.

IDENTITY ACCESS AND MANAGEMENT

Palantir reconciles application and privileged access across the enterprise. By integrating and correlating application access logs, Active Directory records, HR files, VPN activity, authorization systems, and other data sources, Palantir enables analysis of access rights across disparate databases. With entitlements from across the enterprise integrated in a unified environment, CISOs and other executives can pursue data-driven access reduction strategies to reduce both internal and external risk.

ANALYTIC MODULES (CONTINUED)

DDOS RESPONSE

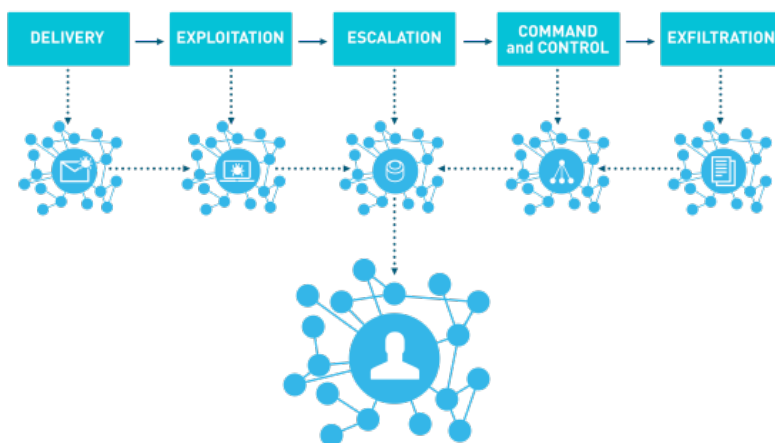
Palantir's scalable data store and knowledge management capabilities provide a reliable corpus of IP data. Users can leverage this data to establish a baseline understanding of expected weblog activity over time to conduct more contextual analysis of incoming threats. Using Palantir's open APIs, organizations can use this intelligence to programmatically modify their perimeter defense strategies and generate automatic reporting on their mitigation and forensic efforts.

FORENSIC INVESTIGATIONS

After data breaches or similar incidents occur, enterprises leverage Palantir to integrate disparate data sources in multiple formats such as computer registry logs, transactions, weblogs, and email traffic databases, creating a comprehensive overview of an incident. Palantir enables analysts to investigate incidents through a framework based on persistent entities, events, and relationships instead of as isolated cases.

APT IDENTIFICATION AND REMEDIATION WORKFLOW

Palantir provides a complete platform for analyzing Advanced Persistent Threats by detecting them at each step in the APT Kill Chain and then correlating behavior across each step to form a composite queue of the highest threat cases. We push the enhanced strategies directly from the Palantir Cyber Mesh and the insights of enterprise security practitioners.



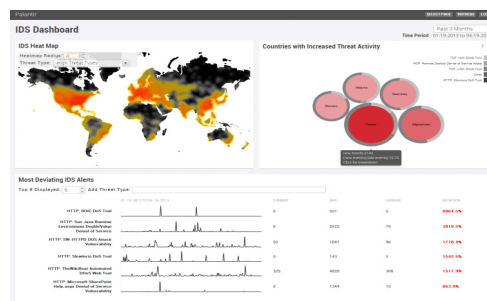
The APT Kill Chain.

ANALYTICAL APPLICATIONS

Palantir Cyber ships with a robust suite of analytical applications out of the box. In addition to the core platform, Palantir’s open architecture allows our engineers and other developers to build custom applications on top of the underlying data, ensuring that the platform can change along with an organization’s evolving mission.

NETWORK DASHBOARDS

Palantir provides a unified data environment and scalable web-based dashboards to visually represent network activity and anomalies. In addition to the full series of dashboards available out of the box, Palantir provides an HTML5-based framework for rapid dashboard customization. Organizations leverage dashboards for a wide range of uses, from providing situational awareness to CISOs and executives to assisting with real-time operations within a Security Operations Center.



A Dashboard presenting notional Intrusion Detection System data.

WEB-BASED IP REPUTATION ENGINE

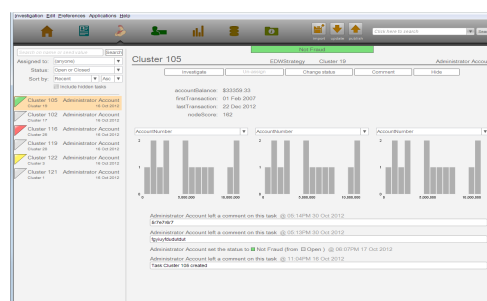
Enterprises are bombarded by IP addresses appearing across network sensors, third party feeds, and peer enterprises. Palantir assesses an IP address’s risk by weighing each disparate source algorithmically. Palantir provides a canonical view of the IP address’s risk via a web-based interface and enables cyber operations teams to make smart and informed decisions within seconds, without having to log in to multiple portals.

The screenshot shows a 'Submit' table with the following columns: IP Address, Threat Score, Reputation, Risk, Category, Category Value, Category, Risk Score, and Risk. The table lists various IP addresses with their corresponding risk metrics.

A web-based interface displaying an IP address’s risk.

PATTERN DETECTION AND WORKFLOW

Palantir Cyber’s Hercules application surfaces threats and incidents amid large-scale structured data. Hercules then algorithmically combs all data sets based on what analysts think are the most relevant criteria, such as behavioral patterns, sets of characteristics, or known entities of interest. The resulting clusters are ranked by relevance and presented with visualizations such as risk scores, pie charts, and heat maps. Modeled after a traditional task management application, the Hercules interface facilitates efficient workflows by allowing analysts to assign owners and statuses to cluster results without having to leave the application.



Hercules presents search results, prioritized for further investigation.



© Palantir Technologies 2013

Palantir Technologies Inc.
100 Hamilton Ave.
Suite 300
Palo Alto, CA 94301

Inquiries: cyber@palantir.com

www.palantir.com/cyber



National Security Archive,
Suite 701, Gelman Library, The George Washington University,
2130 H Street, NW, Washington, D.C., 20037,
Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu