HCP Terminology

Date of Publish: 2018-11-15

http://docs.hortonworks.com

Contents

HCP Terminology

The Hortonworks Cybersecurity Platform (HCP) documentation uses terminology specific to the cybersecurity industry, Hadoop, and the HCP application.

alerts	Provides information about current security issues, vulnerabilities, and exploits.
Apache Kafka	A fast, scalable, durable, fault-tolerant publish-subscribe messaging system you can use for stream processing, messaging, website activity tracking, metrics collection and monitoring, log aggregation, and event sourcing.
Apache Storm	Enables data-driven, automated activity by providing a real-time, scalable, fault-tolerant, highly available, distributed solution for streaming data.
Apache ZooKeeper	A centralized service for maintaining configuration information, naming, providing distributed synchronization, and providing group services.
cybersecurity	The protection of information systems from theft or damage to hardware, software, and the information on them, as well as from disruption or misdirection of the services they provide.
data management	A set of utilities that get data into Apache HBase in a format that allows data flowing through Metron to be enriched with the results. Contains integrations with threat intelligence feeds exposed through TAXII, as well as simple flat file structures.
enrichment data source	A data source containing additional information about telemetry ingested by HCP.
enrichment bolt	The Apache Storm bolt that enriches the telemetry.
enrichment data loader	A streaming or a batch loader that stages data from the enrichment source into HCP so that telemetry is enriched with the information from the enrichment source in real time.
Forensic Investigator	Collects evidence on breach and attack incidents and prepares legal responses to breaches.
Model as a Service	An Apache Yarn application that deploys machine learning and statistical models, along with the associated Stellar functions, onto the cluster so that they can be retrieved in a scalable manner.
parser	An Apache Storm bolt that transforms telemetry from its native format to JSON so that Metron can use it.

profiler	A feature extraction mechanism that can generate a profile describing the behavior of an entity. An entity might be a server, user, subnet, or application. After a profile defines normal behavior, you can build models to identify anomalous behavior.
Security Data Scientist	Works with security data, performing data munging, visualization, plotting, exploration, feature engineering, and model creation. Evaluates and monitors the correctness and currency of existing models.
Security Operations Center (SOC)	A centralized unit that manages cybersecurity issues for an organization by monitoring, assessing, and defending against cybersecurity attacks.
Security Platform Engineer	Installs, configures, and maintains security tools. Performs capacity planning and upgrades. Establishes best practices and reference architecture with respect to provisioning, managing, and using the security tools. Maintains the probes to collect data, load enrichment data, and manage threat feeds.
SOC Analyst	Responsible for monitoring security information and event management (SIEM) tools; searching for and investigating breaches and malware, and reviewing alerts; escalating alerts when appropriate; and following security standards.
SOC Investigator	Responsible for investigating more complicated or escalated alerts and breaches, such as Advanced Persistent Threats (APT). Hunts for malware attacks. Removes or quarantines the malware, breach, or infected system.
Stellar	A custom data transformation language used throughout HCP: from simple field transformation to expressing triage rules.
telemetry data source	The source of telemetry data, from low level (packet capture), to intermediate level (deep packet analysis), to very high level (application logs).
telemetry event	A single event in a stream of telemetry data, from low level (packet capture), to intermediate level (deep packet analysis), to very high level (application logs).