Cybersecurity Situation Awareness

Overview

The Big Data Platform for Cybersecurity Threat Awareness from DP Technology aims to help users detect APT attacks, compromised host, spread of zombie virus, worm and Trojan horse and other security threats, thus enabling accurate traceback and emergency response. Taking network security big data plus AI intelligent analysis technology as the core, the Platform realizes visualization of security event, network-wide threat and traffic, asset and vulnerability, etc. by combining active/passive detection, threat intelligence, UEBA, attack behavior modeling, compromised host detection and other technologies. In this way, it helps customers evaluate their network security status and make decisions on actions. What' s more, the Platform is designed in accordance with GBT-20984-2007, network security Protection System 2.0 and other relevant requirements in order to fully meet compliance requirements.

Product Features

- **Asset Awareness**

  In combination of traffic learning, active detection and an asset fingerprint database, it supports accurate identification of IT assets, including various business systems, IoT terminals, and industrialized devices.

- **Threat Discovery**

  Through a variety of attack detection engines, virus detection engines and threat intelligence, the Platform is capable of detecting high-risk attacks, Trojans and other known threats. AI-enabled detection engines and sandbox detection engines are adopted to discover unknown threats, such as malicious code variants, APT attacks and abnormal behaviors.

- **Risk Determination**

  Correlation analysis is carried out by combining various data sources, including attack logs, asset vulnerabilities, network traffic changes, threat intelligence and third-party security logs, thus effectively determining security events. Based on the results, compromised host can be detected to improve alarm accuracy and reduce false positives. For threat events, full-package traceability of raw data is enabled to ensure accurate traceback.

- **Response and Actions**

  According to customer decisions, security protection equipment can be allocated correspondingly to realize closed-loop disposal.

Specifications

Product Functions	Function Descriptions
Security Event Monitoring	It supports the aggregation and management of various security events such as the spread of zombie virus, worm and Trojan horse, vulnerability exploitation, C&C channel, APT, sensitive information leakage, etc. Further action policies can be developed based on alerts, and hacker archives can also be generated.
Security Threats Analysis	Capable of multi-dimensional and multi-scene modeling, it can perform analysis from multiple dimensionalities, such as internal threats, external threats and outreach threats. It realizes attack traceback by presenting and including attack chain information in relation graph.
Threat Intelligence Correlation	It supports the acquisition of a massive volume of threat intelligence. The data reported by probes can be correlated with threat intelligence in real time, enhancing the ability to detect any indication of advanced threats.
Vulnerability Detection and Verification	Full detection of asset vulnerabilities is enabled on the Platform. In simulation of manual penetration, it performs vulnerability verification, and keeps track of the corrective actions of vulnerabilities to enable closed-loop management.
Abnormal Traffic Analysis	The platform performs regular monitoring on network traffic. Based on self-learning and user-defined models, it is capable of detecting abnormal traffic in the network in an intelligent manner.
Network-wide Asset Monitoring	Asset identification is enabled by combining active scanning and traffic mirroring. Custom labels and weight settings are adopted to realize refined management.
Security Situation Display	The Platform presents network security situation in an all-round manner. Through deep coupling between users' services and industry scenarios, a win-win situation can be achieved both at the macro level of supervision and at the micro level of operation and maintenance.
Actions based on Interactions	A list containing threat addresses prior to any disposal is displayed. According to this list, actions such as blocking, unblocking and ignorance can be taken.

Hangzhou DPtech Technologies Co., Ltd.
Address: 6th Floor, Zhongcai Building, No. 68 Tonghe Road, Binjiang District, Hangzhou City, Zhejiang Province
Postcode: 310051
Official Website: www.dptech.com
Service Hotline: 400-6100-598