Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304

hp.com

News Advisory

HP Threat Central Partner Network Drives Industry Collaboration to Disrupt Cybercrime

Improved defenses through real-time intelligence sharing and analysis uncover attack vectors, methods, motivations behind threats

Editorial contacts

Kristi Rawlinson, HP
+ 1 650 799 7061
kristi.rawlinson@hp.com
www.hp.com/go/newsroom

SAN FRANCISCO, Feb. 24, 2014 — Driving a unified defense to combat cyber threats, HP today introduced the HP Threat Central Partner Network, a collaboration of security vendors who stand behind the importance of threat intelligence sharing across the industry to combat the adversary. Leveraging the HP Threat Central platform, members exchange threat data, analysis and mitigation strategies to disrupt the adversary.

Cyber-criminals have become increasingly sophisticated, sharing resources and techniques to mount increasingly advanced attacks. To beat hackers at their own game, enterprises need a method for sharing targeted intelligence confidentially and in real time to create a unified industry defense.

HP Threat Central, developed with HP Labs, is a collaborative security intelligence platform that enables community members to share threat data and analysis, providing real-time intelligence on the adversaries, attack vectors, methods and motivations behind current threats.

As part of the HP Threat Central Partner Network, HP is initially working with select security vendors including Arbor Networks, Blue Coat Systems, InQuest, ThreatGRID, TrendMicro and Wapack Labs, with plans to bring on additional partners as the program expands. The goal of these relationships is to deliver strategic threat intelligence feeds to provide actionable security intelligence indicators to the HP Threat Central community.

"Adversaries have the advantage today, moving faster, innovating more broadly and organizing around an underground marketplace," said Jacob West, chief technology officer, Enterprise Security Products, HP. "To beat the bad guys at their own game, organizations must collaborate to form a unified defense and that's what HP Threat Central makes possible."

An ecosystem focused on collaborative defense

The advantage of integrating data into a cohesive community in this way means that HP Threat Central members have access to the deep expertise from both HP and a growing network of partners, providing a more robust defense through a single platform.

Members can take advantage of vetted and correlated threat intelligence in an automated fashion through HP ArcSight, HP TippingPoint and other enterprise security products. As the community learns more about a specific attack, the adversary and mitigations, this information can also be made available through an online portal that includes a forum for discussion. Threat intelligence feeds provided by the following inaugural partners will supplement HP Threat Central intelligence feeds and analysis.

- Arbor Networks delivers botnet command-and-control telemetry, sourced from the Arbor ATLAS initiative, directly into HP Threat Central, providing deep intelligence sourced from the ATLAS feed of 70 TB per second of global threat information.
- Blue Coat Systems delivers actionable intelligence on unknown malware and zero-day threats derived from the advanced sandboxing capabilities of the Malware Analysis Appliance to provide a detailed roadmap for remediation and improved defensive posturing by security teams.
- InQuest provides cloud-assisted network threat detection leveraging extensive knowledge of real-world malware campaigns and patent-pending techniques to detect elusive attack patterns that would otherwise go unnoticed. It also identifies, processes and inspects files downloaded over the web or email to detect malicious code in transit.
- ThreatGRID securely crowd sources large volumes of malware and performs advanced analysis in the cloud, or on dedicated local appliances, to identify key behavioral and historical indicators enabling near real-time remediation.
- Trend Micro Deep Discovery provides HP Threat Central customers with enhanced protection against advanced persistent threats and targeted attacks, by detecting the malware, command and control communication invisible to standard defenses.
- Wapack Labs Corp. provides targeted geographic and product-focused security intelligence based on in-house expertise and harvested open source data in the form of non-classified reports to supplement clients' own reporting systems.

In addition to intelligence shared by partners, HP Security Research and HP Enterprise Security Services will contribute intelligence to the HP Threat Central platform. The platform also will feature tight integration with HP ArcSight and HP TippingPoint solutions, providing seamless integration for automated threat download and upload from HP ArcSight Enterprise Security Management (ESM) and automated action (blocking) of malicious IP addresses in the HP TippingPoint Next Generation IPS (NGIPS) and HP TippingPoint Next Generation Firewall (NGFW) devices.

An example of how this could be used is in the detection of malware and the sharing of the remediation across members of the community. One organization might detect malware in their environment, which would be noted in their Security Information and Event Management (SIEM) platform. That information would then be shared through HP Threat Central with other trusted organizations, who could then deploy IPS filters to look for similar behavior in their environments

Pricing and availability

The HP Threat Central beta program is currently available to qualified HP ArcSight ESM customers. Qualified customers interested in participating in the beta program may contact HPTXdev@hp.com.

HP will be showcasing HP Threat Central at RSA Conference 2014 the week of Feb. 24, at booth No. 3401. Additional information is also available at www.hpenterprisesecurity.com.

HP's annual enterprise security user conference, HP Protect, takes place September 8-11 in Washington, D.C.

About HP

HP creates new possibilities for technology to have a meaningful impact on people, businesses, governments and society. With the broadest technology portfolio spanning printing, personal systems, software, services and IT infrastructure, HP delivers solutions for customers' most complex challenges in every region of the world. More information about HP (NYSE: HPQ) is available at http://www.hp.com.

This news advisory contains forward-looking statements that involve risks, uncertainties and assumptions. If such risks or uncertainties materialize or such assumptions prove incorrect, the results of HP and its consolidated subsidiaries could differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements, including but not limited to statements of the plans, strategies and objectives of management for future operations; any statements concerning expected development, performance, market share or competitive performance relating to products and services; any statements regarding anticipated operational and financial results; any statements of expectation or belief; and any statements of assumptions underlying any of the foregoing. Risks, uncertainties and assumptions include the need to address the many challenges facing HP's businesses; the competitive pressures faced by HP's businesses; risks associated with executing HP's strategy and plans for future operations; the impact of macroeconomic and geopolitical trends and events; the need to manage third-party suppliers and the distribution of HP's products and services effectively; the protection of HP's intellectual property assets, including intellectual property licensed from third parties; risks associated with HP's international operations; the development and transition of new products and services and the enhancement of existing products and services to meet customer needs and respond to emerging technological trends; the execution and performance of contracts by HP and its suppliers, customers, clients and partners; the hiring and retention of key employees; integration and other risks associated with business combination and investment transactions; the execution, timing and results of restructuring plans, including estimates and assumptions related to the cost and the anticipated benefits of implementing those plans; the resolution of pending investigations, claims and disputes; and other risks that are described in HP's Annual Report on Form 10-K for the fiscal year ended October 31, 2013, and that are otherwise described or updated from time to time in HP's Securities and Exchange Commission reports. HP assumes no obligation and does not intend to update these forward-looking statements.