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

hp.com

News Advisory

HP Enables Customer Collaboration to Create United Defense Against Cyberattacks

Community-sourced threat intelligence platform automates open sharing of security data to counter advanced cyberthreats

Editorial contacts

Kristi Rawlinson
+1650 799 7061
kristi.rawlinson@hp.com

www.hp.com/go/newsroom

WASHINGTON, Sept. 17, 2013 — HP today announced HP Threat Central, a community-sourced security intelligence platform that will enable automated, real-time collaboration between organizations to combat advanced cyber threats.

The sophistication of cyberattacks has grown substantially in recent years, as adversaries both specialize and share intelligence, tools and plans in order to improperly obtain data and disrupt critical enterprise functions. In isolation, organizations struggle to stay ahead of this new breed of collaborative attacks, placing themselves in constant risk of financial, competitive and reputation losses.

Developed with HP Labs, the company's central research arm, HP Threat Central is a collaborative security intelligence platform for community members to share threat data, analysis and mitigations in order to disrupt the adversary faster and prevent successful attacks.

Currently being piloted with a qualified group of HP ArcSight customers, the platform will provide participants with real-time intelligence on the attack vectors, methods, motivations and specific adversaries behind the threats they face. For example, the banking industry often falls prey to a domino attack where one organization is hit with an attack that is later used against its peers until many have been breached. With HP Threat Central, once a threat is identified, authorized community members are alerted in real time, enabling them to look for similar indicators within their own organizations to get ahead of the adversary.

"Adversaries today organize around an underground marketplace for sharing resources and techniques to mount increasingly advanced attacks that cause extensive damage to organizations around the globe," said Jacob West, chief technology officer, Enterprise Security Products, HP. "To combat collaborative attackers, enterprises must join together by sharing targeted intelligence confidentially and in real time to create a unified industry defense."

Collaboration to disrupt the adversary

In order to counter attacks created by a marketplace of adversaries, organizations must be able to respond quickly and effectively to beat them at their own game. For this to be feasible at scale, the industry needs a common platform that automates the collection and exchange of a broad range of security indicators and threat intelligence in a secure, confidential and timely manner.

Leveraging the platform, community members can submit threat data, analysis and mitigations to which HP will add data and analysis from HP Security Research and partners. Vetted and correlated threat intelligence will then be communicated to members via an online portal that includes a forum for discussion and comments. As the community learns more about a specific attack, the adversary and mitigations, this information will also be shared. Beyond the portal, HP ArcSight customers will be able to automatically leverage shared intelligence to take immediate action.

HP currently analyzes information from a variety of sources, including original research, open source intelligence, as well as active data feeds from HP products and service engagements. The breadth and depth of HP's security assets, install base and security community uniquely positions HP Security Research to facilitate the sharing of intelligence for combating security threats.

"Given the current security landscape, enabling the exchange of threat intelligence between organizations and applying insights gained through sharing are essential to disrupting the growing community of adversaries and minimizing potential business losses," said Christina Richmond, program director, Security Services, IDC. "By integrating shared threat intelligence with HP ArcSight, customers can benefit from rapid, automated response to major threats. This intelligence, vetted by HP and the community, will enable customers to better protect themselves using existing security resources."

HP Security Research conducts innovative research and delivers intelligence to the full portfolio of HP Enterprise Security solutions, giving customers industry-leading protection against the latest threats. Security research publications and regular threat briefings complement the intelligence delivered through HP solutions and provide insight into the future of security and the most critical threats facing organizations today. Leading the company's security research agenda, HP Security Research leverages existing HP research groups, including HP DVLabs and HP Fortify Software Security Research, and manages the Zero Day Initiative (ZDI). Research areas of focus include vulnerability, malware, threat actor and software security with a focus on the technologies, industries and geographies most relevant today.

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 HPThreatCentral@hp.com.

Additional information about the HP Threat Central program is available at HP Threat Central and hp.com/go/hpsr.

HP's annual enterprise security event, HP Protect, is taking place Sept. 16-19 in Washington, D.C.

HP's premier EMEA client event, HP Discover, takes place Dec. 10-12 in Barcelona, Spain.

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; 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 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 Quarterly Report on Form 10-Q for the fiscal quarter ended April 30, 2013 and HP's other filings with the Securities and Exchange Commission, including HP's Annual Report on Form 10-K for the fiscal year ended October 31, 2012. HP assumes no obligation and does not intend to update these forward-looking statements.

© 2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.