July 31, 2019

Intel, Sequretek, Eclypsium and Perception Point Advance Threat Detection Solutions

SANTA CLARA, Calif.--(BUSINESS WIRE)-- **What's New:** Next week at Black Hat 2019 in Las Vegas, hardware and firmware security will be a central topic of conference trainings and briefings. Intel and a growing number of companies in the industry continue to advance technologies that improve security at the lower layers of the computing stack with Intel® Threat Detection Technology (Intel® TDT) that complement built-in capabilities of our Intel® Xeon Scalable platforms for data-center infrastructure and Intel® Core processors for client computing.

> *"In today's cybersecurity landscape, the attackers consistently discover novel attack vectors, exploiting any possible vulnerabilities – in software, firmware or hardware. To support the defense in-depth approach of our customers, Intel has enhanced threat detection at the foundation of the system stack. Our Threat Detection Technology provides security companies with a toolset to augment software-only solutions with hardware-level detectors."*
> – Jim Gordon, Intel general manager of Platform Security

Why It Matters: The threat landscape is constantly evolving, and the rate and pace of security research for software and hardware products continues to accelerate. According to the National Institute of Standards and Technology (NIST), there were 13% more vulnerabilities reported in 2018 than in 2017.

Security solutions need to keep pace with the latest attacks, as well as infinite variations of known attack methods. All of this needs to be done with minimal impact on the customer experience. Intel's hardware-based security technologies deliver two powerful capabilities: accelerated memory scanning and advanced platform telemetry.

How New Intel Customers Use the Technology:

Accelerated memory scanning is an industry enabler: Sequretek* is the latest company to work with Intel to integrate accelerated memory scanning in its endpoint detection, protection and response (EDPR) solution. With plans to release this solution in September 2019, early testing indicates significant performance improvement along with integration of Intel's accelerated memory scanning stack.

Accelerated memory scanning in Intel TDT enables memory scanning that was rarely used due to its effect on system performance and power consumption. Intel offloaded the scanning for memory-based malware from CPU to the Intel integrated graphics processor (IGP). This change allows security solutions to use memory scanning broadly without introducing latency in the customer experience. Today, Intel TDT powers various innovative

security technologies allowing detection of polymorphic malware, file-less threats and crypto miners.

Hardware indicators for advanced threat detection: Eclypsium*, an Intel Capital portfolio company and developer of the industry's first firmware protection platform, announced its plans to work with Intel to advance firmware attack detection with Intel TDT Advanced Platform Telemetry, and deliver a new layer of security that helps defend the enterprise from its computing foundation up. (More from Eclypsium)

Advanced platform telemetry addresses the challenge security software faces to help ensure reliable data feeds detect anomalies or specific behavior below the operating system. Everything that runs on Intel processors generates data from the CPU that can be applied to help detect threats. Intel CPUs can arm security providers with new levels of platform telemetry across PCs and servers to feed machine learning algorithms and improve the detection of advanced threats, while reducing false positives and minimizing performance impact.

Threat detection telemetry creates a framework for continuous innovation: Intel TDT doesn't stop with providing detection techniques. The technology offers a framework to enable security companies to collect various telemetry and indicators from the hardware and create new and differentiated detection solutions.

Perception Point* identified the opportunity to leverage part of this framework in order to dramatically increase visibility into attacks. Its unique detonation environment specifically leverages Intel® Processor Trace (Intel PT), a data source originally developed for debugging as it exposes an accurate trace of activity with filtering capabilities that isolate the trace that matters. Perception Point utilizes Intel PT to record the full execution flow and identify anomalies in the code execution. This is a significant improvement over legacy sandboxes, which lack visibility due to operating at the application level, have latency issues and are limited in scale. Accessing the platform-level data exposed by Intel PT helps enable innovative security companies to better overcome these limitations. (More from Perception Point)

More Context: Media Alert: Intel at Black Hat 2019 and DEF CON 27 | Security News at Intel

About Intel

Intel (NASDAQ: INTC), a leader in the semiconductor industry, is shaping the data-centric future with computing and communications technology that is the foundation of the world's innovations. The company's engineering expertise is helping address the world's greatest challenges as well as helping secure, power and connect billions of devices and the infrastructure of the smart, connected world – from the cloud to the network to the edge and everything in between. Find more information about Intel at newsroom.intel.com and intel.com.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20190731006059/en/

Megan Grasty
Highwire Public Relations
megan@highwirepr.com
916-834-0802

Source: Intel Corporation