Sandia National Laboratories Tracks Hackers and Reverses the Cost of Cyber Crime with Data-Driven Cyber Defense Platform

February 20, 2019

Supported by Splunk, the HADES Program Captures, Monitors and Analyzes Threats by Taking Action on Data

SAN FRANCISCO--(BUSINESS WIRE)--Feb. 20, 2019-- Splunk Inc. (NASDAQ: SPLK), delivering actions and outcomes from the world of data, and Sandia National Laboratories, a national security lab of the U.S. Department of Energy'sNational Nuclear Security Administration (NNSA), are changing the dynamics of cyber warfare by automating threat detection and response. In this case, the Sandia detective work is done in conjunction with the underlying support structure provided by Splunk.

Sandia has launched the High-Fidelity Adaptive Deception & Emulation System (HADES) program, which routes detected threats into a virtual environment designed to emulate real-life networks. HADES enables security analysts to profile adversary movements and automate responses at machine speed, ultimately allowing Sandia to anticipate adversary tactics, better protect networks and save time and money.

As a federally-funded, multi-mission U.S. National Nuclear Security Administration research and development lab, Sandia develops, engineers and tests the non-nuclear components of nuclear weapons, making it a high-value target for cyber adversaries. HADES diverts adversaries with continuously changing targets while offering defenders an undetectable view of attacker movements. Splunk® Enterprise software takes quick action on their data by identifying and analyzing criminal behavior to activate countermeasures with confidence.

“The combined power of HADES using the Splunk Enterprise system enables analysts to run real-time cyber operations that protect our operational networks, while gaining information about the adversaries attempting to penetrate programs,” said Vincent Urias, Distinguished Member of the Technical Staff at Sandia National Laboratories. “As they move about, attackers leave breadcrumbs revealing their steps and the tactics, techniques and procedures that are valuable to prevent future attacks. This one-of-a-kind program can be a model for federal agencies who are struggling to attack and respond to cyber threats at machine speed.”

HADES maps relationships between all relevant parts of an IT ecosystem. With high-precision timestamps, Sandia can sift through data from any source to understand what adversaries are doing, then funnel that intelligence to defenders in real, operational networks. As a result, HADES can deceive, interact with and analyze adversaries in real-time.

“Sending adversaries on the cyber equivalent of a wild goose chase forces bad actors to waste money, time and resources, making cybercriminals incur sunk costs similar to those traditionally experienced only by the defender,” said Frank Dimina, vice president of public sector at Splunk. “Splunk is proud to work with dozens of federal and civilian agencies such as Sandia to tackle their toughest IT, security and IoT challenges head on with data.”

To date, HADES has used Splunk to help Sandia close the threat intelligence gap, as the information gained from HADES is already being redeployed to bolster national security and protection of federal networks.

HADES has garnered acclaim for its highly impactful and important work. Most recently, it was recognized with a Government Innovation Award alongside other celebrated public sector IT disruptors, innovators and emerging leaders.

For more information on how Sandia is using the Splunk platform to redefine real-time cyber defense strategies, visit the Splunk website.

About Splunk Inc.

Splunk Inc. (NASDAQ: SPLK) helps organizations ask questions, get answers, take actions and achieve business outcomes from their data. Organizations use market-leading Splunk solutions with machine learning to monitor, investigate and act on all forms of business, IT, security, and Internet of Things data. Join millions of passionate users and try Splunk for free today.

View source version on businesswire.com: https://www.businesswire.com/news/home/20190220005009/en/

Source: Splunk Inc.

Media Contact
Bill Bode
Splunk Inc.
press@splunk.com

Investor Contact
Ken Tinsley
Splunk Inc.
ir@splunk.com