splunk>

CASE STUDY

Leveraging HADES for Advanced Threat Intelligence

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

Executive summary

As an organization known for its scientific and engineering innovation, it comes as no surprise that Sandia National Laboratories, a multi-mission U.S. National Nuclear Security Administration (NNSA) research and development lab, has developed an advanced approach to address complex national security challenges. Sandia's High Fidelity Adaptive Deception and Emulation System (HADES) is a multi-faceted cyber-defense application that:

- Provides an automation-driven collaborative framework for fast and consistent threat identification and response
- Enables analysts to produce and share threat intelligence while interacting with attacks in real time
- Realizes the ability to deceive adversaries, profiling them incognito to expose their tactics, thereby providing analysts with a significant competitive advantage

Why Splunk

At Sandia National Labs, Vincent Urias, cybersecurity research strategist, supports both externally-focused organizations including the U.S. Departments of Defense and Homeland Security, as well as internally-focused cybersecurity research and development efforts. According to Urias, "We do a lot of test and evaluation. We also look at where the market is, what the gaps are, and try to fill those gaps with proofs of concept and R&D to understand where we need to invest energy, technology and people to mitigate threats or security issues in a broader fashion."

Urias goes on to point out that several years ago, virtualization and newer network technologies were becoming more prevalent in the enterprise; however, understanding adversaries was growing more challenging. The notion of threat intelligence—the ability to identify adversary actions on systems, and then collect, fuse and reconcile that information to create actual intelligence—was a huge gap.

Real-time, real-world threat intelligence

The innovation behind HADES is that it fundamentally rethinks how to address today's adversarial tactics. With a highly instrumented environment, HADES provides deep introspection across all assets—virtual machines, operating systems, network and payload data and any other entity—extracting data in real time about adversarial actions without tipping off the adversary.

Industry

- Public Sector

Splunk Use Cases

- Security

Challenges

- Growing complexity of security threats required advanced threat intelligence to protect national security

Business Impact

- Fast time to value for HADES, with queries up and running in one day
- Threat intelligence spans network, application, service, and operating system indicators – enabling analysts to understand an adversary's command and control
- Gained real-time threat intelligence instead of after-the-fact forensics

Data Sources

- Endpoint
- Firewall
- Operating systems
- Network

Splunk Products

- Splunk Enterprise
- Splunk Enterprise Security
- Palo Alto Networks App for Splunk
- Splunk Add-on for Unix and Linux
- Splunk Add-on for Microsoft Windows

Unlike security tools that rely on historical data for after-the-fact forensics, HADES solves a fundamental deception challenge—fusing human-mediated and machine-assisted deception, live. Analysts are armed with end-to-end visibility and can dynamically determine indicators of compromise (IOCs) to develop profiles of adversaries in real time. These profiles and IOCs can then be used to detect and get ahead of attacks in operational networks, minimizing and in some cases, preventing damage. Furthermore, HADES enables analysts to focus on anomalies and malicious activities that matter by providing contextual enrichment, which is critical for prioritization, reduction of false positives and confident investigations.

"When there is an adversary, looking for password files and using credentials to move around, we want to understand what they are doing and how that actor got into the system," Urias explains. "If you stop the action, you're losing a lot of information about what people were interested in, how much information they had about your enterprise, and what kinds of files they were looking for."

The information collected in the environment provides valuable context about what an adversary is trying to accomplish. Host and network data are correlated under-the-hood through Splunk queries and macros, to create series of Splunk dashboards. Team member William Stout goes on to explain, "We created relationship maps between all of the relevant fields populating our data sources. With high-precision time stamps, we can then temporally step through the events, to tell us everything about what an adversary did, and how they pivoted." Stout continues, "We then use that information to explore what IOCs should be looked for in an enterprise, and format and feed that information to host or network threat detection mechanisms, such as YARA or Suricata."

"We have such complex, non-homogenous data sources in HADES; we were already using the Splunk platform in other areas, so it made sense to leverage it for HADES to meet our needs."

Vincent Urias, Cybersecurity Research Strategist
Sandia National Laboratories

HADES uses the Splunk platform to develop profiles of adversaries, and even detect lateral movement that could take over additional systems. This knowledge helps analysts prepare defenses based on adversarial tactics. Urias and his team are able to stay one step ahead of attacks and disrupt the cost cycle with a solution that shifts the cost to the adversary.

Threat sophistication requires novel approach

According to Urias, the growing sophistication of security threats, including tailored threats, will be a reality for every organization moving forward. Gartner and others have projected that deception and active defense will be important in advancing new security strategies—for everything from a public-sector agency tasked with providing national security to a financial services provider protecting its assets and customer data. These are the impetuses for Sandia's development of the HADES platform.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.