Success Story

US Naval Academy Alumni Association & Foundation Relies on Rapid7 UserInsight for Identifying Compromise and Risky User Behavior

UNITED STATES NAVAL ACADEMY
Alumni Association and Foundation

Industry: Non-Profit
Website: usna.com

CHALLENGE:

In a non-profit organization, cost-effectiveness is essential. The USNA Alumni Association & Foundation needed to build a security architecture to protect personal information of alumni.

SOLUTION:

Rapid7 UserInsight gives situational awareness into users and common attack patterns. UserInsight also provides real-time visibility of compromised user-credentials and world-wide authenticated users, vital for securing the population of remote officers.

Ken Kurz, the Director of Information Services at the United States Naval Academy Alumni Association & Foundation, knows firsthand how difficult it is to make technology purchasing decisions when you work for a nonprofit.

Ken's job is to manage an infrastructure that supports 70,000 living alumni. "Nonprofits cannot leverage government resources," Ken explains, "but at the same time we're a microcosm of any other typical IT shop in most ways."

He certainly has the credentials for the job: Ken spent more than seven years working in information assurance for the NSA, and has also done high-level security engineering and policy work. "I came here to implement a security architecture, and prove that it could be done cost effectively," he says.

Working within the parameters of the nonprofit world, Ken looked to Rapid7 to help "fill in that architecture." From a security standpoint, the most valuable assets on the network are the personal information of alumni. "I need situational awareness of what's going on in my network. And that's where UserInsight factors in."

Rapid7 UserInsight is a solution aimed at detecting and investigating attacks leveraging compromised credentials, user impersonation and lateral attacker movement. When asked about the benefits, Ken's response is simple, at first: "It's about having the right information so that I can build a proper analysis, when necessary."

Then he drills into the specifics.

Discovering Risky Behavior

Security teams work diligently to keep tabs on what's happening across their organization's network. In support of that goal, they must sift through mountains of information to determine which kinds of user behavior are normal, and which kinds are suspicious. This is where UserInsight comes into play - it gives a full picture of activity in one place (rather than scattered across systems) and provides automated analysis to identify anomalous behavior, saving security teams time and improving accuracy.

"UserInsight helps me with data correlation from various feeds. We're not a huge organization, yet we provide service for many, many people. There's a group of us within the IT department, and I fill

"Knowing whose credentials and emails have been exposed is something I absolutely need to know about… Before UserInsight, getting that information was a question of time: I'd have to comb through the data to see whether anyone needed to change their passwords."

—Ken Kurz, Director, Information Services, US Naval Academy Alumni Association & Foundation

the security role – which means I'm going through IPs and trying to get firewall logs and event logs into one place. UserInsight gives me incredibly useful information, like knowing if administrators are creating new accounts."'

In addition to administrator impersonation, UserInsight can also spot other common attack patterns, such as pass-the-hash and harvesting credentials. The solution gives security professionals control over what alerts they see and which they don't.

Where in the World is…

Another of Ken's favorite UserInsight capabilities is the geolocation information, which alerts the security team if there are multiple failed ingress attempts from a location that's not on the normal baseline.

"We have many remote officers traveling around the country," says Ken. "If I see someone logging in from an unexpected location, then I need to know that – and quickly – so I can determine whether it's anomalous. UserInsight enabled me to see who is on our VPN at any given time." The real-time map of user authentication locations also extends to cloud services and mobile devices.

Year of the Password

Passwords, often the weakest link in the chain of security, present tempting targets that all too often can be easily cracked. The Verizon Data Breach Investigations Report found compromised credentials are used in 76% of all network intrusions, a statistic that's been echoed by many headline-making data breaches since Verizon last issued its report.

"When I ran the demo, the first thing that popped up in UserInsight was a series of user credentials," says Ken. "It was telling me that they'd been involved in data breaches." One such alert stemmed from the Stratfor Global Intelligence breach in 2011, when malicious attackers pilfered credit card details, passwords, and home addresses for thousands of clients.

"Knowing whose credentials and emails have been exposed is something I absolutely need to know about – so I can decide whether it's a potential issue. Before UserInsight, getting that information was a question of time: I'd have to comb through the data to see whether anyone needed to change their passwords. Detection of compromised credentials was one of the first features that really made me see what UserInsight could do for us."