SECURITY REPORT

WhiteHat SECURITY

WHITEHAT SECURITY

The AI and Human Element Security Sentiment Study

How Two Powerful Forces Can Tackle Our Biggest Application Security Challenges

Introduction

The convergence of DevOps, Security and Artificial Intelligence is bringing us toward a turning point that nobody can ignore. This year at the RSA Conference 2020, we saw a multitude of industry professionals, once again, coming together to discuss their experience, concerns, and hopes for the future.

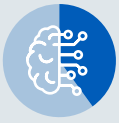
One of our goals here at WhiteHat, is to always stay connected to what is happening in the security industry, and what people are thinking and feeling through their everyday journey. That's why this year, we decided to conduct a survey at the RSA Conference, asking industry professionals specifically what their experience and sentiments were about human expertise and the use of artificial intelligence in identifying and remediating application vulnerabilities.

Report Highlights

1. **Half** of organizations use AI or machine learning in their security stacks

2. **60%** trust findings verified by humans over AI

3. **75%** use an application security tool



4. **40%** of those appsec solutions use both AI and human-based verification

Research Findings

The “AI and Human Element Security Sentiment Study” is based on a survey of 102 industry professionals at the RSA Conference 2020. The research revealed that while over half of organizations use artificial intelligence (AI) or machine learning in their security stack, nearly 60 percent are still more confident in cyberthreat findings verified by humans over AI.

The survey responses, along with the theme of “Human Element” at RSA Conference 2020, reflect the need for security organizations to incorporate both AI- and human-centric offerings, especially in the application security space. Three-quarters of respondents use an application security tool, and more than 40 percent of those application security solutions use both AI-based and human-based verification.

Artificial Intelligence in Application Security

AI and machine learning have provided several advantages for cybersecurity professionals overall the past several years, especially in the face of the technology talent gap, which has left 45 percent of respondents’ companies lacking a sufficiently staffed cybersecurity team.

More than 70 percent of respondents agree that AI-based tools made their cybersecurity teams more efficient by eliminating over 55 percent of mundane tasks. Nearly 40 percent of respondents also feel their stress levels have decreased since incorporating AI tools into their security stack, and of those particular participants, 65 percent claim these tools allow them to focus more closely on cyberattack mitigation and preventive measures than before.

The Human Element is Still Needed

However, a majority of respondents emphasize there are skills that the human element provides that AI and machine learning simply cannot match.

> **Nearly 60 percent are still more confident in cyberthreat findings verified by humans over AI.**

Despite the number of advantages AI-based technologies offer, respondents also reflected on the benefits the human element provides cybersecurity teams.

> **Thirty percent of respondents cited intuition as the most important human element, 21 percent emphasized the importance of creativity, and nearly 20 percent agreed that previous experience and frame of reference is the most critical human advantage.**

Innovation in Application Security

At WhiteHat, we leverage over 150 TB of security data that corresponds to over 100 million attack vectors to drive a very important facet of application security – accuracy of results through vulnerability verification. In doing so, WhiteHat Security engineers and researchers have developed, trained and tested machine learning models that enable increasingly automated vulnerability verification. This automated vulnerability verification allows engineers and researchers the time to develop additional security tests and spend an increasing amount of time in security research that benefits our customers.

The machine learning subsystem is tightly integrated into the WhiteHat Application Security Platform as well as the Threat Research and Operations Center's service delivery process. This allows the Threat Research and Operations Center to govern and evolve the system without disrupting the customer experience. In addition, a subset of vulnerabilities always go through human verification for the following reasons:

1. **To ensure that vulnerabilities that can't be automatically verified by the machine learning subsystem are verified by humans.**

2. **To add new human curated vulnerabilities to the 150+ TB attack vector data lake for future machine learning endeavors.**

3. **For performing quality control on a sample of the automatically verified vulnerabilities and provide a feedback loop to fine-tune machine learning models as needed.**