Automating Threat Detection Desired for Security Analysts Battling Fear of Missing Incidents and Security Operations Center Inefficiency

February 16, 2021

New Voice of the Analysts survey details desire to manage growing alert fatigue amidst flood of false positive alerts

MILPITAS, Calif.--(BUSINESS WIRE)--Feb. 16, 2021-- FireEye, Inc. (NASDAQ: FEYE), the intelligence-led security company, today announced the release of the IDC InfoBrief “The Voice of the Analysts: Improving Security Operations Center Processes Through Adapted Technologies”. In surveying 350 internal and managed security service provider (MSSP) security analysts and managers, the report finds that security analysts are becoming less productive due to widespread “alert fatigue” resulting in ignored alerts, increased stress, and fear of missing incidents. To improve job satisfaction and effectiveness, the report also uncovered the top activities analysts felt would be best to automate to better secure their Security Operations Centers (SOCs).

“Security analysts are being overwhelmed by a flood of false positive alerts from disparate solutions while growing increasingly concerned they may miss a true threat,” said Chris Triolo, Vice President of Customer Success at FireEye. “To solve these challenges, analysts are asking for advanced automation tools, like Extended Detection and Response, which can help reduce the fear of missing incidents while strengthening their SOC’s cybersecurity posture.”

Security analysts continue to feel the pressure of increased alerts, spending almost half their time on false positives.

- **False positives create “alert fatigue”:** While analysts and IT security managers receive thousands of alerts every day, respondents indicated 45 percent of the alerts are false positives, making in-house analysts’ jobs less efficient and slowing workflow processes. To manage alert overload in the SOC, 35 percent of this group said that they ignore alerts.

- **MSSPs spend even more time sifting through false positives, and they ignore more alerts:** MSSP analysts indicated that fifty-three percent of the alerts they receive are false positives. Meanwhile, 44 percent of analysts at managed service providers said they ignore alerts when their queue gets too full, which could lead to a breach involving multiple clients.

Fear of missing incidents (FOMI) is impacting a majority of security analysts and managers.

- **As analysts experience more challenges managing alerts manually, their worry of missing an incident also increases:** Three in four analysts are worried about missing incidents, and one in four worry “a lot” about missing incidents.

- **Yet, this FOMI is plaguing security managers even more than their analysts:** More than 6 percent of security managers reported losing sleep due to fear of missing incidents.

Analysts need automated SOC solutions to combat FOMI.

- **Less than half of enterprise security teams are currently using tools to automate SOC activities:** Respondents shared the top tools they use to investigate alerts, showing that less than half use artificial intelligence and machine learning technologies (43 percent), Security Orchestration Automation and Response (SOAR) tools (46 percent), Security Information and Event Management (SIEM) software (45 percent), Threat Hunting (45 percent), and other security functions. In addition, only two in five analysts use artificial intelligence and machine learning technologies alongside other tools.

- **To manage their SOCs, security teams need advanced automated solutions to reduce alert fatigue and improve success by focusing on more high-skilled tasks like threat hunting and cyber investigations:** When ranking the activities that are best to automate, threat detection was the highest (18 percent) on the analysts’ wish list, followed threat intelligence (13 percent) and incident triage (9 percent).

Additional Report Resources

- FireEye blog post with additional report analysis, “Avoid Fear of Missing Incidents with Automation and XDR”

IDC InfoBrief Methodology

IDC surveyed 300 IT security managers and security analysts in the U.S. working in SOCs across multiple verticals including financial, healthcare, and government, as well as 50 managed security service providers on the challenges they experience managing their SOCs. The survey was conducted in Fall 2020.
This IDC InfoBrief was previously sponsored by Respond Software, now a part of FireEye.

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 9,900 customers across 103 countries, including more than 50 percent of the Forbes Global 2000.

© 2021 FireEye, Inc. All rights reserved. FireEye and Mandiant are registered trademarks or trademarks of FireEye, Inc. in the United States and other countries. All other brands, products, or service names are or may be trademarks or service marks of their respective owners.

View source version on businesswire.com: https://www.businesswire.com/news/home/20210216005436/en/

Media:
Media.Relations@FireEye.com

Investors:
Investor.Relations@FireEye.com

Source: FireEye, Inc.