

Sai Huda's best-selling book Next Level Cybersecurity reveals signals missed in world's largest hacks such as SolarWinds

The ground-breaking book reveals 15 signals and a seven step method to detect the hack in time and prevent loss or damage

SAN DIEGO, CALIFORNIA, UNITED STATES, March 1, 2021 /EINPresswire.com/ -- Even with more than \$100 billion spent each year on security, attackers continue to break in through the front door or a backdoor, stay hidden, steal valuable data or disrupt with ransomware.

Just take the recent case of SolarWinds, where the hack was one of the largest in history with hundreds of organizations world-wide compromised in one fell swoop by inserting a backdoor malware in the supplier's software update process. As each SolarWinds customer downloaded the update, they unknowingly downloaded the backdoor that allowed the attackers to break in, spy and steal sensitive data.

The attackers remained undetected for over nine months until FireEye, a customer of SolarWinds discovered the backdoor and brought to light the hack. Could the hack have been detected early and loss or damage prevented?

"With a high degree of confidence, I can say that the SolarWinds attackers could have been detected early if one was looking for certain signals. In my book, [Next Level Cybersecurity](#), I reveal the top 15 signals of attackers and a seven step method to detect the hack early and prevent loss or damage," said Sai Huda. "Intensive research of dozens of the world's largest hacks confirm there will be a pattern of signals of the attackers in each step."

"In the SolarWinds case, there were at least four of the 15 signals that could have detected the attackers in time. These 15 signals are time tested because they focus on attackers common behavior once they are in, regardless of whether they came in the front door or a backdoor," continued Huda.

"Let's face it, the attackers will get in. The question is not if, but when? So the key to success in cybersecurity is to cut thru all of the noise and find certain signals in the network to detect the attackers before it is too late," said Huda.

In the game-changing book, [Next Level Cybersecurity: Detect the Signals, Stop the Hack](#), the

reader will:

- Learn the Top 15 signals of cyber attackers' behavior and activity;
- Understand how these signals can detect the attackers;
- Discover how these signals were missed and could have detected the attackers in the world's largest hacks, such as SolarWinds;
- Find out how supply chain, cloud and Internet of Things (IoT) are danger zones, and know what signals to look for;
- See how to implement the signals in seven steps — with this method, detect the attackers early, stop the hack and prevent damage.

Sai Huda is a globally recognized risk and cybersecurity expert, technology visionary and business leader, with more than 20 years of hands-on experience.

He served seven years as General Manager, Risk, Information Security and Compliance Solutions at Fidelity National Information Services, Inc. (FIS), a Fortune 500 company serving more than 20,000 clients globally. Under his leadership, FIS attained number one ranking in RiskTech 100.

Prior to FIS, he was the founder and CEO of Compliance Coach, Inc., an innovative risk management software and consulting services company, focused on compliance, operational and information security risk management, serving more than 1,500 clients in financial services, healthcare and government sectors. Compliance Coach was acquired by FIS.

He serves as an expert consultant to boards and executives on risk and cybersecurity best practices. He is a founding member and on the advisory board of Cyber Center of Excellence (CCOE), a non-profit organization dedicated to promoting cybersecurity best practices and job growth in the cyber economy. He is also a frequent keynote speaker at industry conferences. To learn more, visit www.saihuda.com.

Sai Huda

www.saihuda.com

info@saihuda.com

This press release can be viewed online at: <https://www.einpresswire.com/article/535950517>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2021 IPD Group, Inc. All Right Reserved.