# Lessons learned: Back to the Basics

Debby asked me to share my lessons learned after my blog post *Summary of SolarWinds breach for InfoSec noobs* went viral on LinkedIn. At the time of writing, this post has almost 12k views, 186 reactions, and 52 comments. This is unexpected for a LinkedIn user with only 300 connections.

The first thing I asked myself after reading Debby's message was: Why did this specific blog post become so successful? How could an information security greenhorn like me attract so much attention from information security novices and experts alike?

On my website, which I created in October 2020, I blog about information security. Each time I publish a new blog entry, I advertise it on LinkedIn as well. My blog focuses on technical topics, like endpoint analysis or penetration testing. *Summary of SolarWinds breach for InfoSec noobs* was the first entry that tackled a topic of general interest. This seems to clarify why this post attracted more interest than any of my other articles but still does not explain why it went viral on LinkedIn. The only thing I was sure about is that the success of this blog post was not random. The next step was to pinpoint the features that made it so well received.

I published *Summary of SolarWinds breach for InfoSec noobs* on December 15th, that is, two days after FireEye published the report about the malware SUNBURST. The cybersecurity company headquartered in Milpitas, California, uncovered a campaign with which threat actors gained access to numerous public and private organizations around the world via trojanized updates to SolarWinds' Orion IT monitoring and management software.

Between December 13th and 15th, I read many articles about the SolarWinds hack. Some of these articles were very technical and thus inaccessible to the layperson, whereas others did not cover all the important aspects of the breach. This is when I made it my duty to write a summary of the breach for information security beginners.

My blog post explains the SolarWinds breach by answering eight fundamental questions:

1. Which company develops and sells the compromised software?
2. Which software was compromised and what does this software do?
3. What happened exactly?
4. What is the possible impact?
5. Which are some US institutions using Orion?
6. Who are the malicious actors? What is their goal?
7. How did SolarWinds get breached?
8. How many governments and companies have been compromised?

The structure of the blog is loosely based on the "5Ws + H"[1] formula used in journalism, that is, the journalism basics. According to the many comments written below the related LinkedIn post, the clear structure and the layperson language used to describe that facts are the secrets behind the success of *Summary of SolarWinds breach for InfoSec noobs*.

All in all, the key to explaining a complex subject such as the SolarWinds breach to a general audience is to break down a topic in its most basic components and explain those components in non-technical language.

Michele Pariani

[1] 5Ws + H: Who, what, when, where, why, how.