VIAVI Solutions

Case Study

# Remediation After Sunburst Cybersecurity Incident

**Organization:** Large global technology company headquartered in California.

## The Problem

The organization was running SolarWinds Orion instances across their IT estate. They needed to quickly ascertain the impact and their exposure due to the SUNBURST hack of December 2020.

**The Background:**

The IT team was running VIAVI Observer platform in multiple strategic datacenters around the world. The IT networking services team were also using SolarWinds Orion software. The production services were running a version of SolarWinds Orion that did not contain the vulnerability. A second, non-production demo instance, was built in June 2020 for a 30-day trial period to explore new features. That instance did contain the vulnerability.

## Business Goals

The key goal was to understand if any confidential or sensitive data had been accessed or exfiltrated. This was of particular concern given the nature of the solutions provided by the organization concerned, as reputational damage would have long-term consequences to current and future business relationships.

## Solution

The immediate response was to quarantine the demo instance whilst continuing with investigations based on the guidance from SolarWinds, CISA and other Cybersecurity agencies. Investigations were performed per recommendations using their centralized firewall logging SIEM and Network flow data analysis tools.

VIAVI Observer Platform was used as an additional layer of monitoring and an important forensics tool to validate historical traffic flows to and from the SolarWinds server.

The Observer solution provided details:

a. Dating back to the time of the known attacker compromise at SolarWinds, of network traffic flows and packet level data for forensics.

b. With any attempts made, from inside the organization borders, to any of the more than 500 command and control hosts in published resources.

c. Observer GigaFlow can show any attempted activity to blacklisted IPs from anywhere that it is monitoring, not just the Observer server.

d. Visibility into all traffic to and from the vulnerable SolarWinds Orion server.

## Results

Using VIAVI Observer forensics, the organization was quickly able to confirm no evidence of exploitation or activation of the vulnerability. Their Cybersecurity team is staying on top of new information and implementing additional recommended protections. VIAVI Observer platform will continue be a critical tool to monitor and investigate issues on their networks.

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact


techco-cs-ec-nse-ae
30192965 900 0221