How to remediate SolarWinds with Skybox: step-by-step guide

On December 24, 2020 SolarWinds issued an advisory detailing a cyberattack to their systems that inserted a vulnerability (SUNBURST) within the Orion® Platform software builds for versions 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF 1, which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run. Hundreds of thousands of SolarWinds customers including US government agencies might feel the ripple effect of this enormous attack on the supply chain. At Skybox, we immediately updated our Vulnerability Dictionary and posted information about the vulnerabilities on our Vulnerability Center.

Our solutions for Vulnerability and Threat Management and Security Policy Management help to identify and remediate vulnerable assets. These solutions, combined with the recommended best practices below, can help prevent similar attacks in the future.

Step 1: Discovery of SolarWinds instances with Skybox Vulnerability and Threat Management:

What we do:

- Awareness of the newly discovered vulnerability – Skybox can give visibility into the new announced vulnerabilities including general details, CVSS, related sources, affected platforms/versions, associated malware/exploits, solutions, external sources, and threat history. We can set notifications on key technologies used by specific organizations to give an early warning in the event of newly discovered vulnerabilities. This is all powered by Skybox's Threat Intelligence Feed.

- Discovery – Our proprietary algorithms aggregate across existing data sources, such as vulnerability scanners, to show reported occurrences linked to the Vulnerability Definition.

- Analysis – In the absence of vulnerability scan data, we can deduce the existence of the vulnerabilities and the devices where they are found via patch/CMDB data.

Here's how to do it:

Using asset inventory data collected by Skybox, you can identify which of your servers have SolarWinds installed and what version is running in your environment

1. In the Java client, go to the Model workspace
2. Right click on Model Analysis, and create a new Analysis
3. Give the analysis a name (IE: SolarWinds Services) and click on the ellipse to the right of Product
4. In the search field, type SolarWinds and click Search. Select all the SolarWinds results returned and click the right arrow, followed by OK to close the search window, then OK again to save your analysis and view the results

Step 2: Immediate Mitigation with Skybox Security Policy Management

To perform immediate mitigation, ensure that SolarWinds servers are isolated / contained until a further review and investigation is conducted. This should include blocking all internet access from SolarWinds servers.

Here's how to do it:

1. Leveraging the Skybox Model, run a Network Access Analysis (from "any" to the SolarWinds servers and vice versa) to identify the current access and validate what needs to be done to restrict it

If the SolarWinds infrastructure is not isolated, consider taking the following steps:

2. Restrict scope of connectivity to endpoints from SolarWinds servers, especially those that would be considered Tier 0 / crown jewel assets -> Run a Network Access Analysis (from SolarWinds to the Endpoint networks) to identify the current access and validate what needs to be done to restrict it
3. Restrict the scope of accounts that have local administrator privilege on SolarWinds servers.
4. Block internet egress from servers or other endpoints with SolarWinds software. -> Run a Network Access Analysis (from the affected servers/endpoints to "any") to identify the current access and validate what needs to be done to restrict it.

Consider conducting a review of network device configurations for unexpected / unauthorized modifications -> Run Change Tracking and Configuration Compliance

analysis to validate if/when/what/who made any change to network devices. Also, consider network zoning and ensuring compliance with Skybox Access Compliance.

Step 3: Prioritizing instances for remediation (with Skybox Vulnerability and Threat Management)

Using Skybox, you can quickly map vulnerability spread and density throughout organizational units and across geographies. By doing so, you will be able to identify hot spots where intensive triage is needed. Analyze potential attack paths and business impacts to prioritize the remediation according to imminent and potential threats. Metrics to determine the risk include asset importance (as defined by the customer), network accessibility of the vulnerability (Exposure), CVSS score, and exploitability:

- Exploitability — correlate vulnerability data with exploit availability and use.
- Exposure — security teams can run "attack simulation" from third party connections to see if the organization could potentially be infected remotely from those connections — and then close the connections to prevent a second and third cycle of contamination.

Here's how to do it:

1. Click on Prioritization, within the Vulnerability and Threat Management web interface, then Vulnerabilities.
2. Create a new Filter Set specifically for CVE ID CVE-2020-14005
3. Ensure Risk Score is selected in the Sort By field.

Following these steps, customers will be able to prioritize vulnerabilities based on the highest risk to their organization. The filter sets can also be used for widgets and customized dashboards.

Step 4: Ongoing Remediation and Tracking (with Skybox Vulnerability and Threat Management)

Skybox will suggest the most relevant remediation options: apply patches (e.g. SolarWind's recommendation to upgrade Orion Platform to 2019.4 HF6, 2020.2.1 HF2, or later), implement IPS signatures, workarounds and access rules to block attack paths. This functionality enables you to address imminent threats first and deal with potential threats over time:

- Use the Skybox remediation center to track the remediation status for SUNBURST or other imminent threats. Make sure there is no “long tail” of machines that have not been fixed.
- Receive up-to-date information regarding new remediation options as they become available within time.
- Track progress and analyze trends to find areas that need more attention or resources.
- Monitor remaining vulnerabilities for changes in exposure or use in the wild.

10 steps to preventing a similar attack in the future

In addition to the full lifecycle vulnerability and threat management steps outlined above, Skybox advisors recommend that organizations continue to enforce cybersecurity best practices:

1. Build and maintain a detailed understanding of the assets within your network, including cloud and virtual networks, aligned to business criticality using the Skybox Security Platform and suite of products

2. Change your approach from simple vulnerability management to threat-centric vulnerability management:

    a. Conduct a comprehensive risk assessment of all vulnerabilities in your network, including cloud and virtual, using Vulnerability Control

    b. Prioritize vulnerability remediation by "imminent" and "potential" threats using Vulnerability Control; develop a plan to remediate imminent threats immediately and track through to completion; deal with potential threats over time

3. Address underlying issues around poor cyber hygiene immediately:
    a. Disable any single-factor login entry points
    b. Validate patching and hardening processes
    c. Segment critical data and assets and increase defenses around these areas

4. Rehearse and revise incident response playbooks

5. Update security tools to include detection signatures released by FireEye or any other pen testing vendor to identify exposed red team tools

6. Perform regular retroactive threat hunting activities on the past several weeks' data focusing on irregular VPN logins, windows native scripting and authentication activity

7. Identify and audit your network perimeter to ensure ingress/egress is properly identified; understand the extent of access that all third- parties have into your network using Network Assurance and Firewall Assurance

8. Audit network and firewall infrastructure regularly for misconfigurations using Firewall Assurance and Network Assurance

9. Build compliance and risk assessment into firewall change processes using Change Manager

10. Develop fit-for-purpose organizational access policies and configuration standards using Firewall Assurance and Network Assurance

Additional resources:

Visit the Skybox Vulnerability Center to keep up-to-date on your vendors' and products' vulnerabilities >

Read the Risk-based Vulnerability Management eBook to discover how Skybox reduces risk of attack within some of the world's largest organizations >

Read the Intelligent Vulnerability Prioritization Solution Brief to discover how to leverage insight to improve your security posture >

About Skybox Security

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of dynamically changing attack surfaces. At Skybox, we don't just serve up data and information. We provide the intelligence and context to make informed decisions, taking the guesswork out of securely enabling enterprises at scale and speed.

Our security posture management platform delivers complete visibility, analytics and automation to quickly map, prioritize and remediate vulnerabilities across your organization. The vendor-agnostic platform intelligently optimizes security policies, actions and change processes across all corporate networks and cloud environments. With Skybox, security teams can now focus on the most strategic business initiatives while ensuring enterprises remain protected.