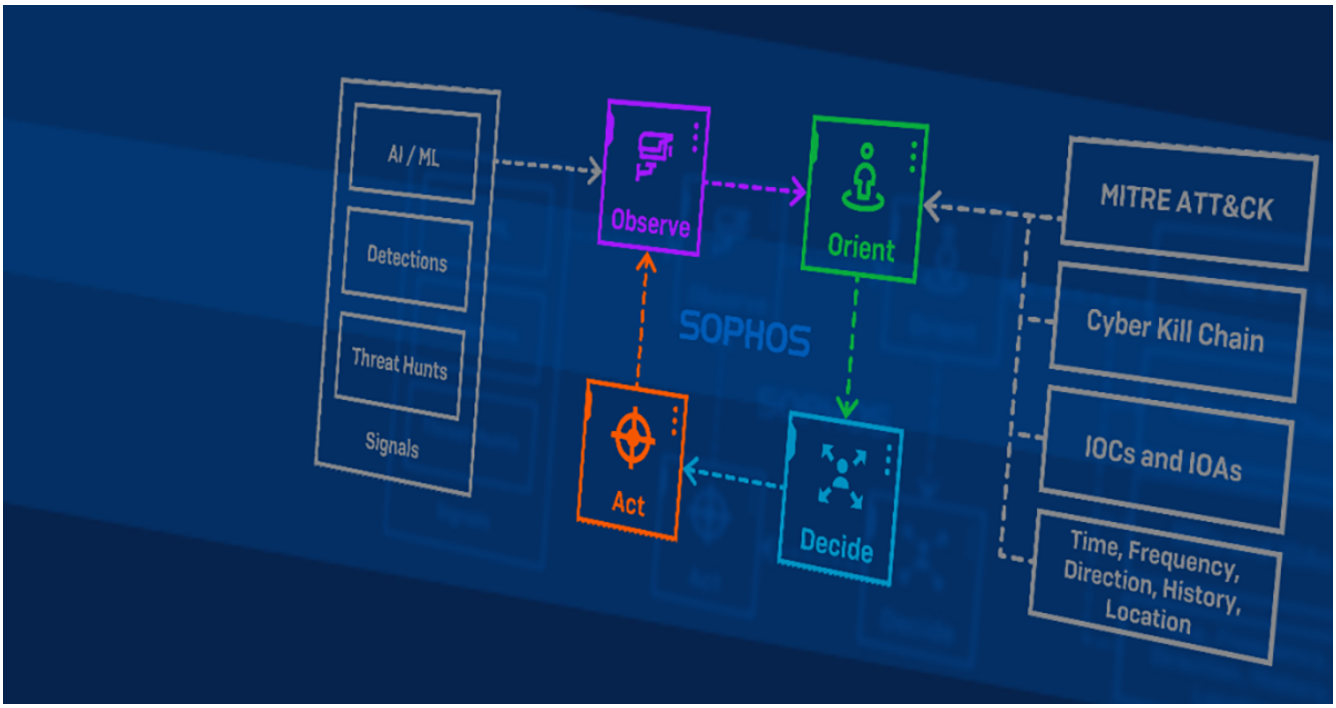
# Incident response playbook for responding to SolarWinds Orion compromise

news.sophos.com/en-us/2020/12/14/solarwinds-playbook/

Ross McKerchar December 14, 2020




*** We will continue to update this article with additional information as it becomes available. Check back here and GitHub regularly for further updates. ***

*Last updated 2020-12-15T12:18Z – view the changelog below*

For security teams who have SolarWinds in their environment looking to initiate incident response, we're providing the following playbook, based upon our initial understanding of the threat, as an aid to help you investigate any potential attack. The information presented may not be complete or eliminate all threats, but we expect will be effective based on our experience. As more information becomes available about the threat, recommended steps may change or be updated.

## Example threat model

This response process may need to be customized for your environment and is based upon the following assumptions:

1. Ability to establish when the vulnerable component was introduced into the environment and log coverage for that period.
2. Assume adversary had access to all accounts and credentials utilized by SolarWinds Orion server and the capability to assume the identity of any administrative or related accounts.
3. Assume adversary had the capability and network access to maintain a C2 channel to SolarWinds Orion server.
4. Ability to determine that no accounts used by SolarWinds, nor accounts used to access the SolarWinds Orion server had full domain administrative rights.

5. Ability to determine that no active malicious activity occurred relating to the vulnerable component based upon currently available IOCs and detections.

*If you find evidence of malicious activity or if you are not able to arrive at some of the baseline conclusions described here, Sophos recommends initiating your full incident response procedures or reaching out for external assistance.*

## Detection and analysis

## Hunt for impacted SolarWinds instances

### Endpoint queries

**Sophos EDR/Osquery:** Detection queries

**Sophos Intercept X:**

Sophos Application Control detects all versions of SolarWinds Orion as “SolarWinds MSP Agent”. Application Control is an optional setting – read the Help Guide for instructions on how to enable it, and add SolarWinds to the list of apps you want to block.

Labs detections: List of detections and IOCs

**Manual (example):**

PS C:\Windows\system32> Get-FileHash C:\Orion\Solarwinds.Orion.Core.Businesslayer.dll | Format-List

Algorithm: SHA256

Hash: CE77D116A074DAB7A22A0FD4F2C1AB475F16EEC42E1DED3C0B0AA8211FE858D6

Path: C:\Orion\Solarwinds.Orion.Core.Businesslayer.dll

### Network queries

SolarWinds can be detected via network monitoring by looking for call-homes made by its updating service. The following Zeek IDS searches may also help: SIEM Searches.

*Note: You may only see outbound connection from your main SolarWinds instance not pollers.*

## Identify malicious SolarWinds components

### Endpoint indicators

Warning: check your configuration for exclusions.
See https://twitter.com/ffforward/status/1338785034375999491

**Sophos Intercept X / Central Endpoint Protection**:

SophosLabs contains both detections for the malicious component and the additional signature that indicate active exploitation. Sophos has also blocked all associated IP and domain indicators for its customers. See GitHub for detection names.

**Sophos EDR/OSquery**: Detection queries

### Network indicators

Sophos has also blocked all associated IP and domain indicators for its XG and SG customers. If you have additional network telemetry the following searches may also be of use: SIEM Searches

*Note: The attacks communicate to C2 via TLS so a file hash hit is unlikely unless you intercept TLS.*

## Prepare for forensics

If possible, snapshot all affected hosts with impacted versions of Orion installed.

Ensure that snapshotting processes also capture memory.

- VMware: https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.html.hostclient.doc/GUID-A0D8E8E7-629B-466D-A50C-38705ACA7613.html
- Hyper-V: https://support.citrix.com/article/CTX126393

A lightweight forensic acquisition can also be performed using the “Forensic snapshot” feature of Sophos EDR.

## Scope potentially compromised accounts

Potentially impacted accounts are:

1. All accounts SolarWinds used for network monitoring, this includes Windows local accounts, domain accounts, SNMP, SSH, etc.
2. All other accounts used on the affected SolarWinds Orion Servers. These include all administrative logins (e.g. EventCode 4624) to the server and any local or service accounts. (e.g local SQL database account.)

The following table can be used to document all potentially impacted accounts:

| Username | Desc | Protocol | Domain | Domain Admin | Server admin/root | Scope | Notes |
|---|---|---|---|---|---|---|---|
| (fully-qualified username/UPN) | Brief overview of what it’s used by | Windows/KRB/NTLM \| SNMP \| SSH etc | | (y/n) | (y/n) | What hosts this is applicable to | |

## Identify high-value attack paths for potentially compromised accounts

For all potentially compromised accounts listed above, identify other high-value systems (e.g. domain controllers, Active Directory Federation Services, and Azure Active Directory Connect servers) to which they had access.

1. Evaluate local system authentication logs for anomalous activity from compromised accounts.
2. Bloodhound can also be used to map out access of any potentially impacted accounts.

If servers or accounts involved in federated authentication (e.g. ADFS servers) were potentially impacted, refer to Microsoft's customer guidance and develop an appropriate additional containment strategy.

## Containment and eradication

Warning: these steps assume a desire to preserve the environment for further forensic investigation and may have an impact on production environments.

1. Isolate all SolarWinds Orion instances from the network:
    1. Instant isolation can be performed at the host level using such controls as Sophos EDR via Sophos Central.
    2. Host-based isolation should be backed up by network–based isolation. Systems should be migrated to an isolated non-routable VLAN with console access only (migrating to a VLAN helps preserve network state for future forensics).
2. Perform credential reset or disable and recreate all potentially impacted accounts:
    1. Important: Ensure that no fresh or reset accounts are used to access any compromised infrastructure.
3. Rebuild fresh monitoring servers from known-good sources ready for release of Orion platform version 2020.2.1 HF 2, which is planned for release on Tuesday, December 15, 2020.
4. Consider taking forensic snapshots and rebuilding additional exposed hosts, including:
    1. Any hosts running the SolarWinds agent.
    2. Any hosts for which potentially compromised accounts had access rights.

## Changelog

2020-12-15T12:18Z Added warning about checking your configurations for exclusions