

Tracking Sunburst-Related Activity with ThreatConnect Dashboards | ThreatConnect

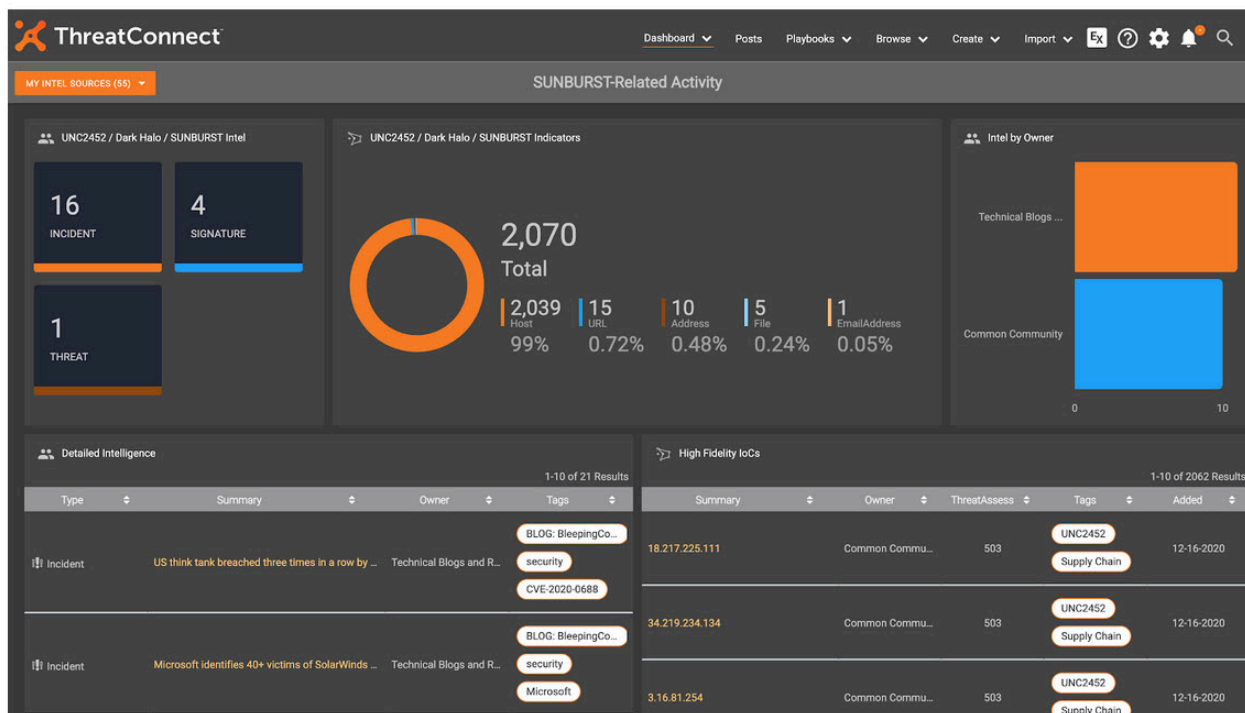
By ThreatConnect

Published: 2020-12-18 · Archived: 2026-04-05 15:37:17 UTC

Recently FireEye discovered that the SolarWinds Orion IT monitoring platform was compromised earlier this year. The threat actor used SolarWinds cryptographic keys to sign multiple backdoored files posing as Orion IT updates. These files contained a hidden backdoor that would communicate via HTTP to external servers after remaining dormant for up to 2 weeks. The malware disguised communications as legitimate data being sent to SolarWinds.

The number of organizations affected by this malware is what makes the attack remarkable. SolarWinds estimates approximately 18,000 customers installed these malicious updates, including private sector organizations, the US Departments of Treasury, Commerce and Homeland Security.

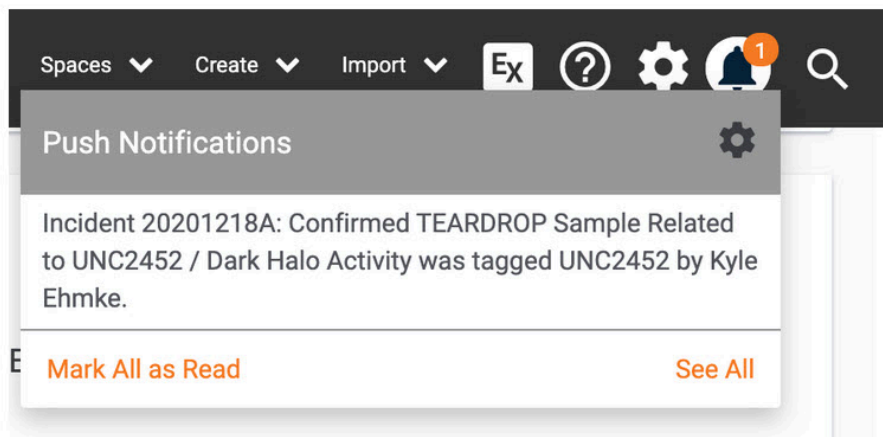
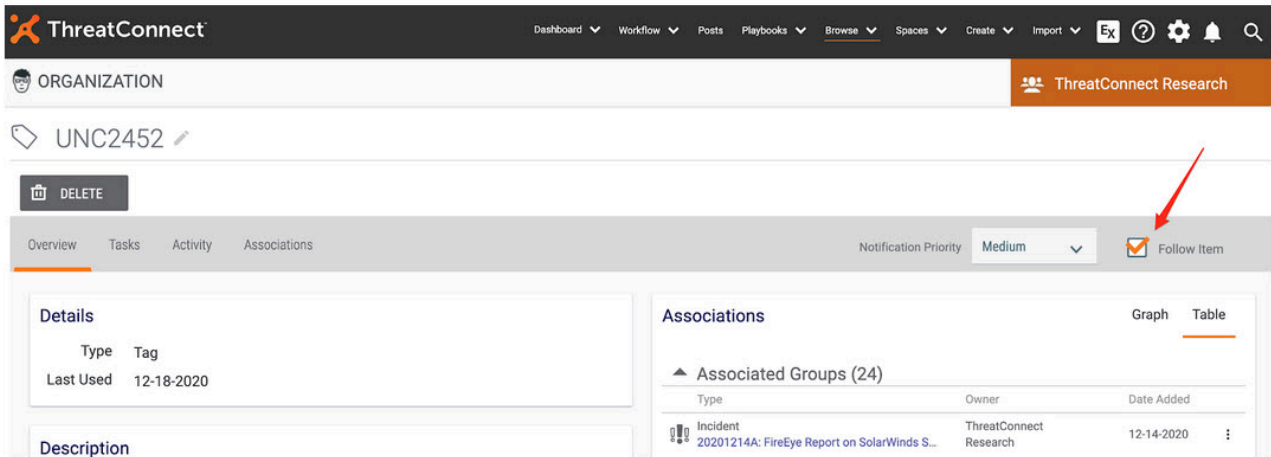
Available immediately to ThreatConnect users is a Dashboard that provides a single location to view relevant intelligence and indicators of compromise (IOCs) from across various sources related to the SolarWind event. The Dashboard helps consolidate intelligence that would otherwise take a large amount of time to identify in separate sources. Public Cloud users can now access a [SUNBURST-Related Activity Dashboard](#) by choosing clicking that link or navigating to ‘Dashboard’ and choosing it from the drop down.



A Glimpse of the Activity Displayed on the SUNBURST-Related Activity Dashboard

For our customers leveraging our dedicated cloud or on-premises deployment options, the ThreatConnect Customer Success Team has built out instructions on how to create this dashboard in your own, private instance. Find a write-up outlining this process and how to create the necessary Dashboard cards in the [ThreatConnect Learning Management System](#).

In addition to the Dashboard above, for individuals and organizations looking for proactive alerts to new intelligence and indicators related to this activity, ThreatConnect provides the Follow capability. Following tags like UNC2452, Dark Halo, or SUNBURST can generate an alert in the platform or to your email when that tag is applied to an indicator or group.



We hope that this information helps you answer some of the difficult questions around this recent series of attacks. Beyond just this specific instance, remember that you can modify these queries to create topical dashboards around whatever your high priority threats might be. TQL is your language for situational awareness.

About the Author

ThreatConnect

By operationalizing threat and cyber risk intelligence, The ThreatConnect Platform changes the security operations battlefield, giving your team the advantage over the attackers. It enables you to maximize the efficacy and value of your threat intelligence and human knowledge, leveraging the native machine intelligence in the

ThreatConnect Platform. Your team will maximize their impact, efficiency, and collaboration to become a proactive force in protecting the enterprise. Learn more at www.threatconnect.com.

**Subscribe
to our Emails**

Source: <https://threatconnect.com/blog/tracking-sunburst-related-activity-with-threatconnect-dashboards>