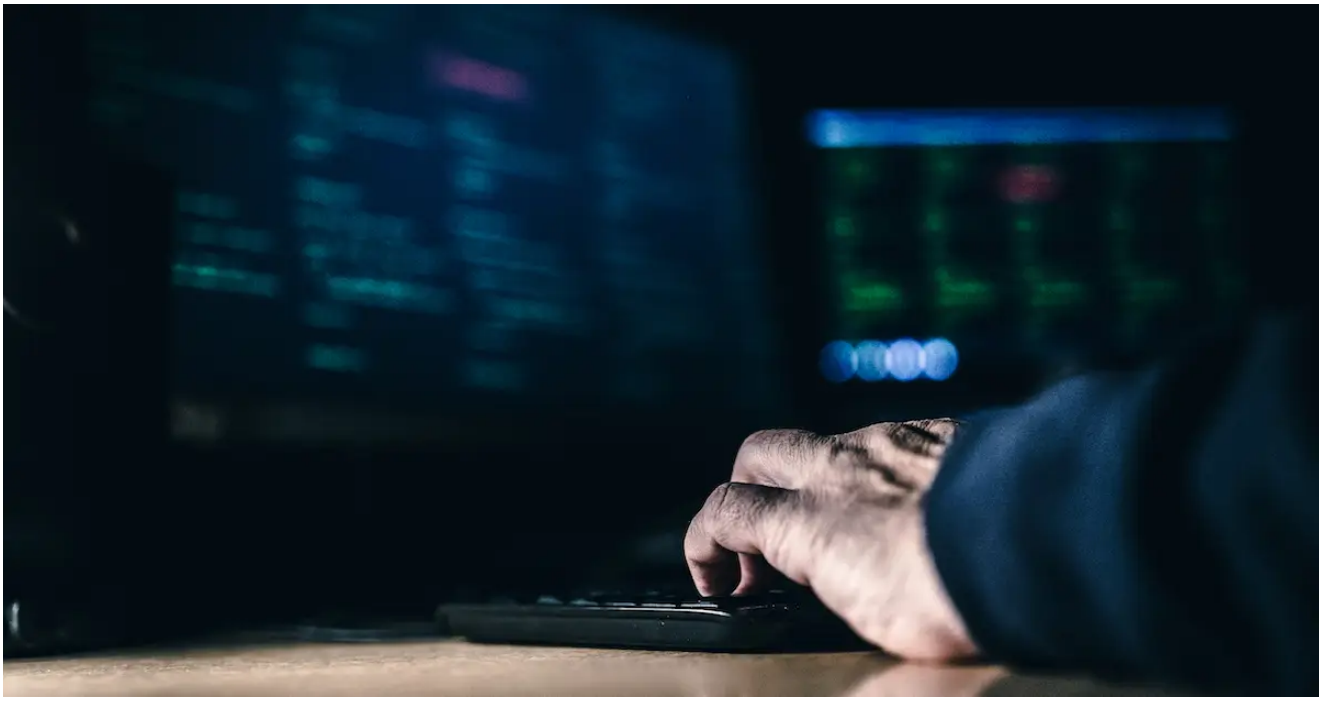
Combating Sleeper Threats With MTTD

securityintelligence.com/articles/sleeper-threats-mean-time-to-detect/



Advanced Threats April 16, 2021

By Koen Van Impe 6 min read

During the SolarWinds Orion supply chain compromise, threat actors lurked in the victim's network for more than a year. Discovered by FireEye in December 2020, the earliest traces of a modified SolarWinds Orion go back as early as October 2019. Although these early

versions did not contain the malicious backdoor (this was added in March 2020), it means attackers were able to remain hidden for a long time. This sleeper threat affected corporations and government agencies around the world. To counter these, we need to be aware of mean time to detect (MTTD) and mean time to response (MTTR) when detecting this kind of attack.

To pull off such a long-lasting con, the attackers required a high level of refinement and planning. That's something you associate with an advanced persistent threat (APT). These APTs, often launched by nation-states or state-sponsored actors, are stealthy and strive to remain hidden for a long time. (Contrast this with hacktivists, who often intend to make a visible statement, like internet graffiti.) APTs choose their targets carefully and tread as lightly as possible until they reach their final goal.

These objectives are often political or economic. They go beyond the financial gain sought by those who deploy ransomware. And while single components of these attacks are maybe not considered advanced, their operations and planning are top notch. When they do attack, they avoid interrupting business since that would give away their presence. In a later stage, they can still decide to push the destruct button, though. For example, they might want to cover up tracks, as revenge or a statement.

Sleeper Threats

The global median dwell time, or the number of days before an intrusion is detected and the threat is neutralized, was 56 days in 2019. These 56 days already provide ample time for attackers to do their work. What about the fact that 12% of the investigations had dwell times greater than 700 days? This provides plenty of chances to access confidential data, exfiltrate secrets and cause financial and legal harm.

Before jumping into specifics on how to reduce this dwell time, let's look at the performance metrics to describe the time to detection and response.

MTTD and MTTR

MTTD is the average time it takes for your security team to discover an incident. This metric can be found by adding up the total time it takes to detect incidents and dividing that by the number of incidents. The mean time to detect covers three phases. First, you collect event data, then apply some logic to this data to discover strange behavior. As a final step, do an assessment to determine if the activity is indeed a threat.

Meanwhile, MTTR measures the average time it takes to contain and repair a threat. (Sometimes this is also referred to as the mean time to recover.) The mean time to respond follows when your assessment indicates there is a likelihood of a threat. Your team then looks at the data to determine the exact nature and impact of the incident. Following this, you can start repairs to neutralize the intrusion.

The MTTD and MTTR metrics can serve as a barometer for the strength of your defenses. Shortening the MTTD and MTTR and stopping an attack not only limits the impact of a breach and prevents loss of money and standing, it also prevents legal harm. For example, the Network and Information Security (NIS) Directive and the General Data Protection Regulation (GDPR) require timely notifications of incidents.

So, how can you lower the dwell time and reduce MTTR and MTTD?

Reduce the MTTD

One of the essential elements for detecting attacks is not really that novel. It's about having fine-grained insight into what's happening in your landscape. You can do this by employing targeted log management. Make sure the logs contain information that is actually helpful when spotting strange events. Then, centralize the collected logs, events and alerts. Use them for correlation, such as in a SIEM. In addition, you can use network sensors that capture network packets and flows, and use end-point alert and activity tracking.

Collecting the data is only the first step in reducing the MTTD. The sheer volume of data is most likely staggering. There are always too many alerts and not enough time to chase them all. To make things worse, defense teams have to work with different tools, confusing user interfaces and different event formats and log types. Wading through all the data to do an assessment is impossible. How can we cut out these obstacles and assess if a certain event poses a real threat?

The answer lies in using automated incident response to reduce the dwell time, often referred to as SOAR. This automates routine investigative tasks and automatically launches responses when an alert is detected, greatly reducing the MTTR. It completely removes the time needed to inform analysts and wait for a human follow-up, which also greatly reduces MTTD and MTTR. A SOAR system can interact with different tools and then provide a single overview pane for your analysts. This type of integration cannot happen overnight, though. Start small, assess what works within your environment and extend your model with more sources.

Take a proactive approach to threats

Define 'Normal'

Automation requires you to do some prep work. First, you need to set a baseline and define what is normal. This alone can already be very challenging. But if you want to identify potential sleeper technology hiding in your environment, you need to know what's likely and what's unlikely in each case.

- Start from a base image installation and find the installed programs, running services and the typical system utilization.

- Profile not only the behavior of systems and apps but also the behavior of users. For example business hours, device usage, volume of files accessed and internet usage.
- Baselining the network traffic helps to identify odd ports and protocols. It also highlights abnormal packet sizes, suspicious volumes of transferred data or lengthy connections.
- Understand which domain names your group commonly uses. Isolate domain names that are used by only a couple of devices or users or only during specific timeframes.

Visualize All Things

Another good method is visualizing the event and alert data of your environment. Although visualizing performance indicators have their merits, they are only a subset of what's important to represent in dashboards. Other items to include are:

- Event, log and alert timelines
- Events matching with threat data
- VPN and network usage by protocol, sources, destinations, port usage, length of connection and volume
- Domain name analysis
- System and service activity
- User activities on multiple or different systems in a short timespan, including lateral movement of users between systems
- New devices, apps, services and processes
- Changes in roles, users, groups and group memberships
- Logon activity, failures, logouts and credential changes
- File volume and user file activity

Security Monitoring With MTTD

Although a large portion of the alerts can be handled via your automated responses, you still need a team of specialists to monitor what's happening. They can use the centrally collected alerts, events and visualizations to spot anomalies. This team, often in the form of a security operations center, plays a crucial role in looking after your environment, responding to alerts and reducing the MTTD. The playbooks help them to execute this response in a consistent and uniform way.

As in the case of the SolarWinds attacks, the threat actors aren't ordinary 'script kiddies'. Some of the threat groups have their foundation in traditional espionage and can be very determined to breach your environment. Stopping just one technique or putting a halt to a first intrusion doesn't make these groups give up. They'll just attempt another approach. Automation, baselining, visualization and monitoring is not your only answer to reduce the MTTD and uncover the activity of these groups.

Improve Your MTTD Maturity

Another important element is to improve and work on the maturity of your team in an ongoing manner. The Security Incident Management Maturity Model is a good guide to improving your incident detection and response capabilities. This framework focuses on organizational aspects such as establishing a sufficient set of policies and having a governance framework. An important aspect of this is to create robust incident response plans and document the roles and responsibilities in your incident response workflow. These incident response plans also serve as the basis for your playbooks, which then steer the automated detection and mitigation.

People are still the driving force behind a well-functioning detection and response program. Ensure that your incident response plans take into account the way departments work together and talk among themselves. Carefully sort the workflows between different teams to prevent snags.

Training and regular exercises help your team to stay alert and practice their skills. Your security team must understand the incident response processes and have insights into common attacks, threat actor techniques, and best practices for how to defend against them. Focus on these key points in trainings:

- Determine how reliable and accurate the information received from your detection capabilities is. Train your team to understand the blurry areas and explore those that do not always provide conclusive information.
- Which weaknesses can you find where actors can bypass detection?
- Train your team to be fluent in making records of their findings, and use this to improve playbooks and plans.
- Document other steps required to confirm or deny false positives.

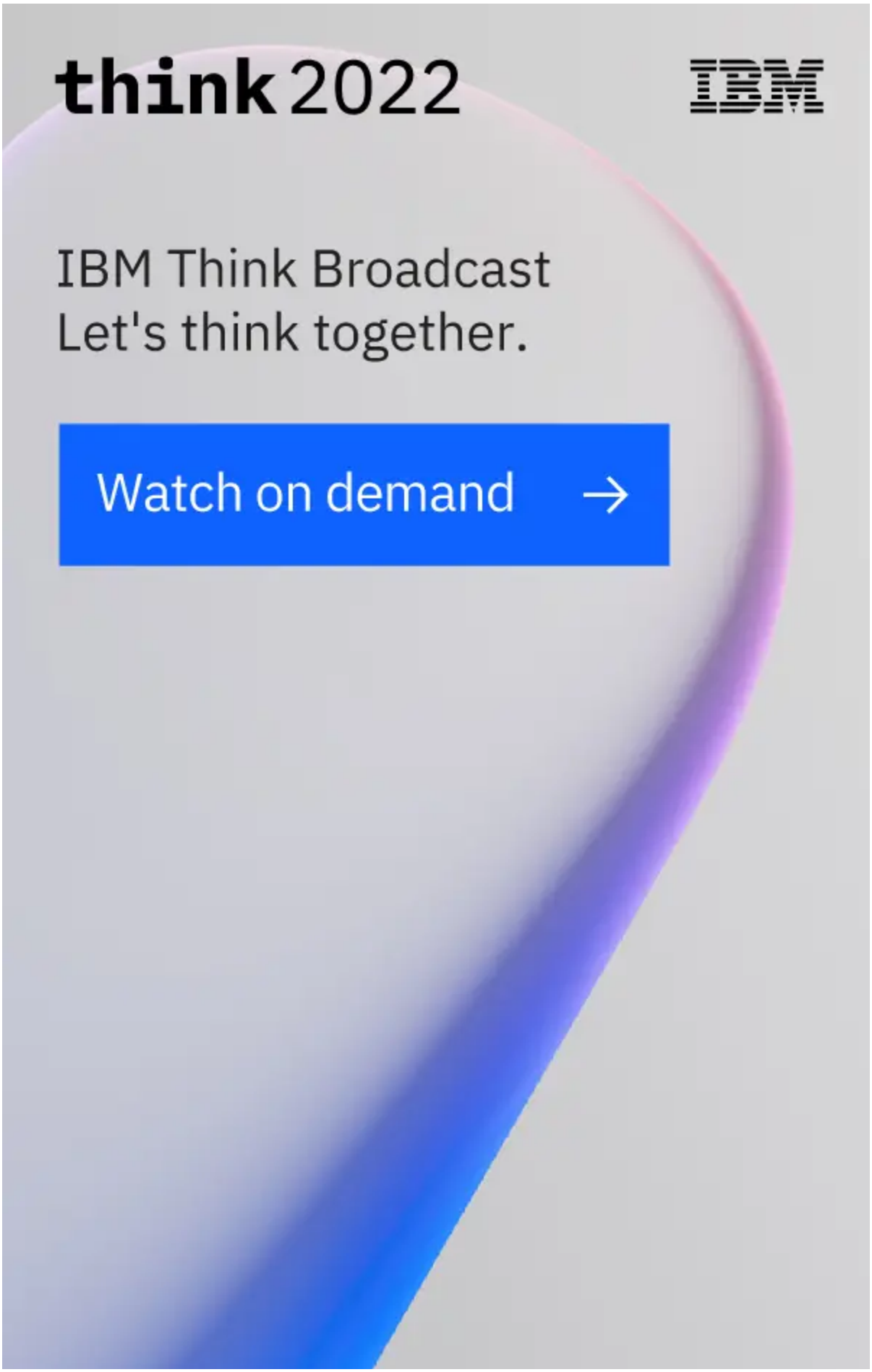
What's Next for MTTD?

Because attackers keep improving their game, you'll have to make sure you keep up with them. There is, however, a limit to what you can do with alert-based monitoring to reduce the MTTD. We already covered baselining and using it to detect anomalies in system and user activities. But there's more. You can also use machine analytics and implement scenarios based on real life tools, techniques and procedures to improve your workflows and anomaly detections.

In the end, the key is to extend your detection capabilities with a well-functioning threat intelligence platform that can look out for sleeper threats in your sector.

Koen Van Impe
Security Analyst

Koen Van Impe is a security analyst who worked at the Belgian national CSIRT and is now an independent security researcher. He has a twitter feed (@cudes...


think 2022
IBM
IBM Think Broadcast
Let's think together.
Watch on demand