11:00:52 From Tyler Mortensen : snowboarding is better than skiing :P

11:01:37 From Tyler Mortensen : Very true. It is very difficult

11:05:34 From Nathan Stien : Q: did they ever get a thing that can ingest Prometheus format metrics? :-)

11:06:18 From Nathan Stien : I >1 GB per day of Prometheus data you can ingest at some point

11:08:20 From Joshua Durst : Q; Maintenance mode for systems, are system admins going to be able to self manage those in the future?

11:10:39 From Adam Listek : Q: Can you set those maintenance modes through an API call or PowerShell?

11:10:58 From Bill Hamann : Yes, Adam.

11:11:04 From Kevin Selinger : Q: But wasn't it turning off the 24/7 monitors the issue for not sending alerts?

11:11:18 From Adam Listek : Thanks Bill :)

11:11:51 From Jason Mays : Q: How do we go about setting up custom application monitors and can we leverage PowerShell Scripting as described in https://documentation.solarwinds.com/en/Success_Center/SAM/Content/SAM-Create-Windows-PowerShell-Script-Monitor.htm

11:12:20 From Kevin Selinger : No mic, sorry

11:15:01 From Kevin Selinger : That explains it Mike as my experience was with the custom port 443 alert for vsphere.ilstu.edu

11:15:51 From Bill Hamann : oh, my!

11:17:46 From Bill Hamann : Okay, that's understandable. it would be nice to document what such requests would look like

11:18:12 From Bill Hamann : as time allows. So we don't waste your time, and vice versa.

11:19:59 From Bill Hamann : Okay, I envision us testing a custom monitor ourselves based on your guidance, and so when we think it's good, we would pass it on, and you could turn it around it quickly without much fuss.

11:20:16 From Tony Brook : That might be something we can leverage the test system for. :)

11:20:26 From Bill Hamann : that sounds good!

11:21:24 From Bill Hamann : Could we please get the samples from C:\Program Files (x86)\SolarWinds\Orion\APM\SampleScriptMonitors, as time allows.

11:21:44 From Tony Brook : On my list. :)

11:22:04 From Ballard McCleskey : At one point, the main goal was to replace and expand on monitoring and alerting that we were getting from SCOM. Now that has been accomplished, how much have the vision and goals evolved for the future. [Things we have decided to do, and things we are considering/evaluating]

11:22:05 From Bill Hamann : cool! And sounds good, Michael

11:25:49 From Michael Knerr : Bill: Getting those script samples should be no problem

11:26:16 From Nathan Stien : for the time being, my team is using Prometheus Alerting (per Red Hat) to construct integration-related monitors but we'll happily switch to Orion for that when it becomes feasible. our current ones are all just time series queries against metrics data.

11:26:27 From Ben Mengarelli : Q: What kind of training do you offer for those new to Orion?

11:26:56 From Ballard McCleskey : The history of SolarWinds/Orion is much longer than the last week!

11:27:07 From Ben Mengarelli : https://ithelp.illinoisstate.edu/knowledge/7137-overview-of-the-orion-platform/

11:27:08 From Bill Hamann : true!

11:27:17 From Ballard McCleskey : Yes Tony, that answers the question - thank you!

11:29:16 From Bill Hamann : favorite colors?

11:29:29 From Tony Brook : Purple. :)

11:29:47 From Tony Brook : (I could change the overall color scheme of Orion, but we don't want to do that for accessibility reasons)

11:31:02 From Nathan Stien : is that selenium based?

11:31:18 From Tony Brook : It is not, unfortunately.

11:31:34 From Tony Brook : (and yes I've asked Solarwinds to support Selenium imports)

11:32:05 From Majeed Abu-Qulbain : There will be quite a bit more "end to end" style monitoring requests, especially around idm flows (is replication happening in a timely manner?, password updates, etc), sso flows.

Its similar to the custom monitor convo from earlier, but it will be interesting to see how (or what has been done so far) external automation tech that is currently in place can tie in to orion alerting. What types of mods are needed? Log to file and have orion watch it? What else?

```
11:32:23   From  Tim Flynn : Have we tried Application monitoring from nodes outside of ISU's network?
11:32:53   From  Michael Knerr : Tim: We do have some application monitors using agentless polling.
11:34:31   From  Nathan Stien : we have some "a thing didn't happen for X period of time" alerts related to integrations, and these work by checking the presence of metrics data generated by our integrations data flow engine (Apache Camel)
11:37:43   From  Colten Keeling : is Orion just for monitoring, or can it initiate commands somehow also? such as in Jason's idea for having a PowerShell Script doing the monitoring, could that same method be used to say : "Start a service if said service is found 'stopped' for X minutes?"
11:38:14   From  Adam Listek : You're talking about remediation, that would be handy
11:39:59   From  Bill Hamann : yes, we should! To keep them honest!
11:40:16   From  Adam Listek : Or at least ingest the results from there to make a single pane
11:40:36   From  Bill Hamann : good question and thought, Tim.
11:44:17   From  Bill Hamann : no wonder why Orion was a target
11:44:28   From  Kevin Selinger : and I can assure you I've kicked the orion service account from vSphere so there isn't a threat there.
11:44:43   From  Tony Brook : Which we appreciate. :)
11:44:44   From  Bill Hamann : Thanks, Kevin!

11:47:02   From  Bill Hamann : yes!
11:47:03   From  Nathan Stien : InfoSec twitter has been real good the past couple days
11:47:03   From  Adam Listek : Absolutely!
11:47:10   From  Tyler Mortensen : Yes, very informative.  Thanks!
11:47:16   From  Eric Grab : Yes, thanks.
11:47:45   From  Robert Oakley : Great presentation Tony and Mike!
11:48:42   From  Bill Hamann : Yes, great job, Tony and Mike.  And good conversation all!
11:49:04   From  Tim Flynn : Alert fatigue.
11:49:32   From  Adam Listek : Control has always been an issue, that's why SCOM never took off for us in many ways. Having the ability for us to do as many operations as possible is important.
11:49:40   From  Tim Flynn : No.
11:50:05   From  Nathan Stien : with prom, it batches multiple related alerts into a single notification and this in itself cuts the fatigue considerably
11:50:24   From  Bill Hamann : sound good
11:50:48   From  Kevin Selinger : I think solarwinds already changed their best practices to say no direct WAN access
11:51:00   From  Nathan Stien : sometimes when an integration fails it fails thousands of times per second
11:51:12   From  Adam Listek : That was the same problem with SCOM, which is why we ultimately didn't use it because we needed custom monitors for virtually everything.
11:52:29   From  Eric Grab : That sounds nice.
11:53:33   From  Bill Hamann : with the good working relationship and the formalized request process, we'll realize the dream this time
11:53:50   From  Adam Listek : Yep, I'm not knocking, and Bill will drive that dream for us here :)
11:54:23   From  Bill Hamann : oh, yeah, all's good.
11:55:19   From  Kevin Selinger   to   Tony Brook(Direct Message) : https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Good article about it if you wanted to share with everyone if they're curious
11:56:09   From  Colten Keeling : 10/10 would attend again :)
11:56:11   From  Adam Listek : Great job!
11:56:17   From  Dongli Zhang : Thank you!
11:56:20   From  Bill Hamann : Thanks all!
11:56:21   From  Majeed Abu-Qulbain : Thanks much guys!
11:56:22   From  Mike Mansfield : Thanks for the presentation, gentlemen! Great work.
11:56:24   From  Eric Grab : Thanks.
11:56:31   From  Tyler Mortensen : Thanks!
11:56:31   From  Joshua Durst : Thanks! Well done
11:56:34   From  Nathan Stien : <fry from futurama meme>
```

shut up and take my metrics data