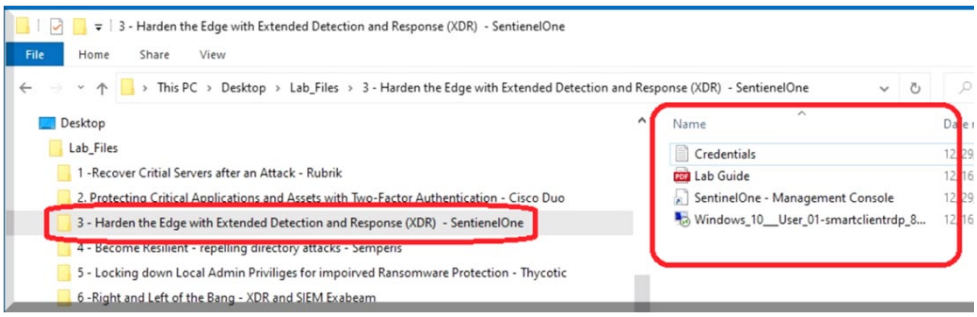
Welcome to Lab #3

This event is guided by instructors, but you may wish to refer to this guide during or after the event has completed.

Orienteering

Objective:

- Get familiar with the environment
- Login to the SentinelOne Management onsole and explore



<- Your desktop has the file structure that covers this lab, #3 for SentinelOne.

<- This folder has various files that will help you during the lab.

- Credentials: Username/password and link to the SentinelOne Management Console
- Lab Guide: This guide
- SentinelOne Management Console: URL shortcut to the management console
- Windows10_UserXX-smart client: RDP link to a virtual machine used during lab

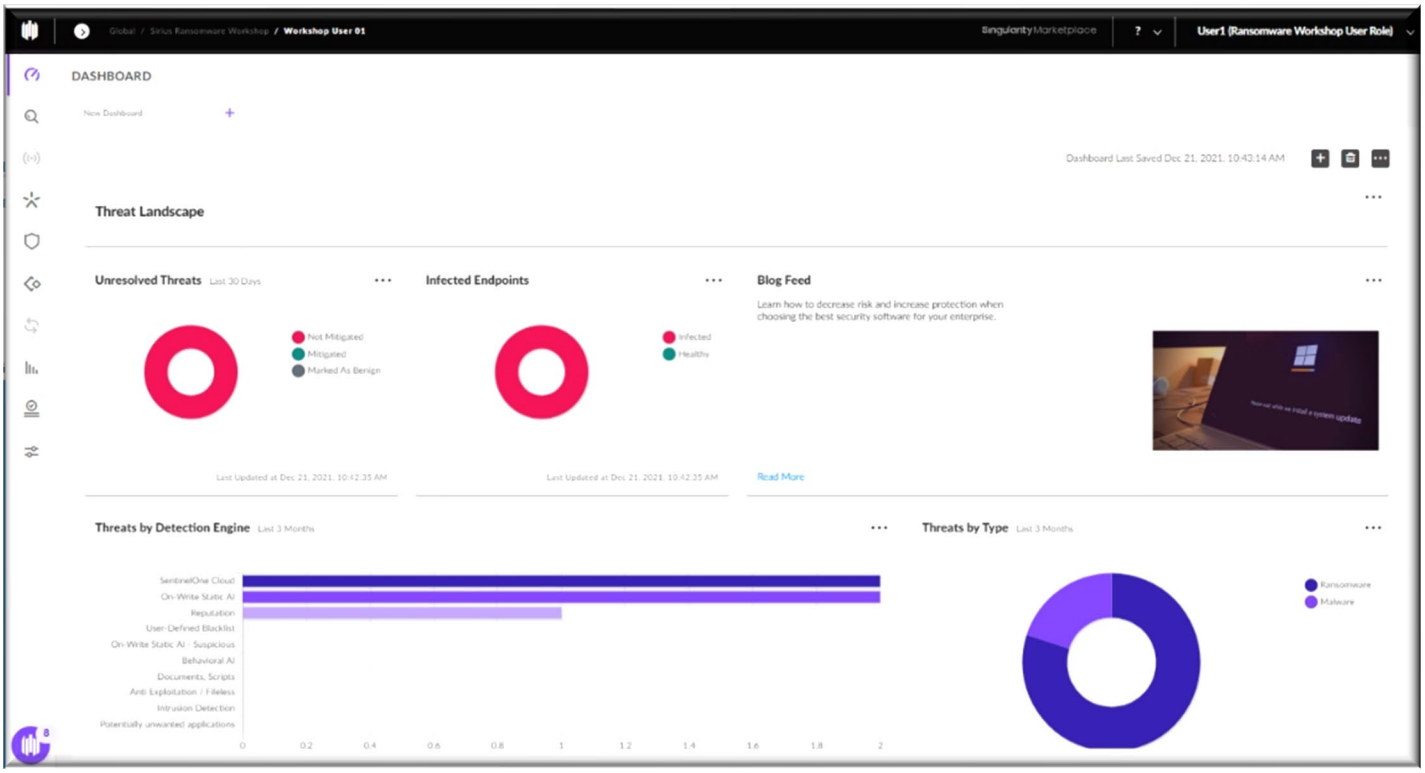
<- You should be able to click the HTML short cut for access to the Management Console. If not, the URL is listed below and contained in the TXT file “Credentials” on the lab machine itself.

Step One:

Login to console: usea1-300-nfr.sentinelone.net

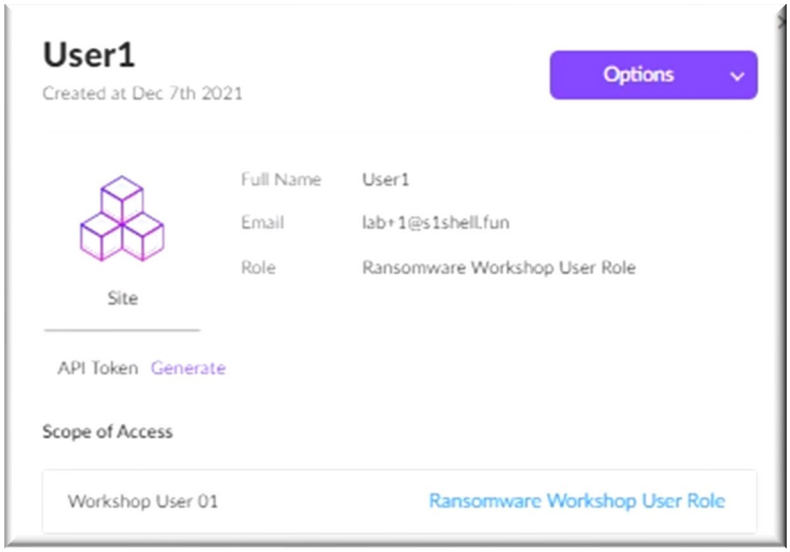
Use the lab credentials you received for the day: lab+X@s1shell.fun ← where X is the number assigned to you for today’s lab. So if you were assigned #9 today and you logged into the virtual desktop with “sid-sec9” this morning, then your username to access the SentinelOne Management console will be “lab+9@s1shell.fun” (yes the “+” is part of the user name).

Explore the console (stay on dashboard)



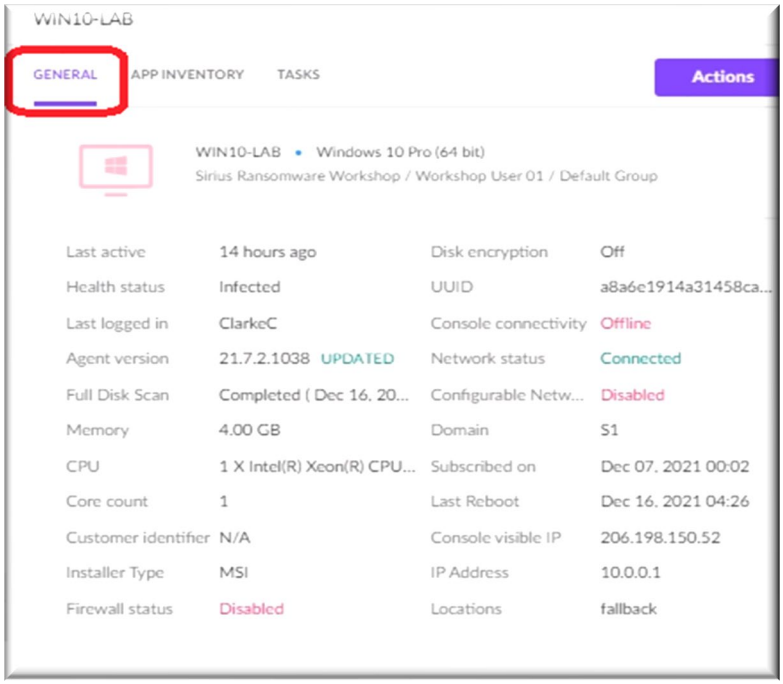
Take a moment to review what is on the main dashboard that comes standard with SentinelOne. Your dashboard may look slightly different but this gives you an idea of the information that is represented.

Task one: Which user are you? Can you tell? Bring up the details on your user account



SentinelOne allows granular levels of access and permissions within our organization. This gives the ability to designate operations and responsibilities to various groups or departments but maintain overall control of the organization.

A basic concept of SentinelOne is a site, which is an easy way to create hierarchy in the SentinelOne installation. It contains objects to deploy polices to a group, as well as define access for users via the site level. Think of a site as a scope of access to resources.

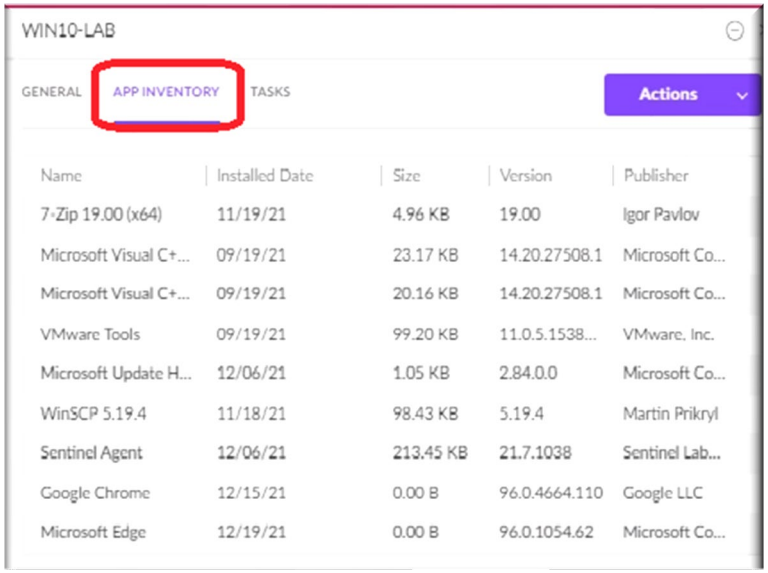


Find your device: In the SentinelOne side menu, locate the WIN10-LAB device.

Review the details about this device, including hardware, network settings and current connectivity.

What other types of information is shown in this summary tab?

- Health status
- Agent version
- Firewall status
- Console connectivity



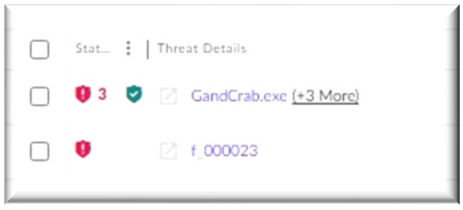
As you move along the top menu, we can even get a list of installed software with install dates and versions. This can be useful information to have about the state of devices in a ransomware outbreak.

The last tab “TASKS” probably does not have any current tasks being run on it, at the start of this lab.

Task 2: Let’s look at the incidents.

This is where activity can be tracked throughout your environment. In the early portion of the lab, this will be mostly empty. But that is going to change soon. Take a minute to look at the information on-screen.

Incidents (shield) will show the incident activity in your environment that you have scope to see. You can see from a high level if things are in a state of resolved/unresolved, where they are occurring, and how many indicators there are currently. Can you determine at a quick glance which events are “resolved” vs. on-going issues?



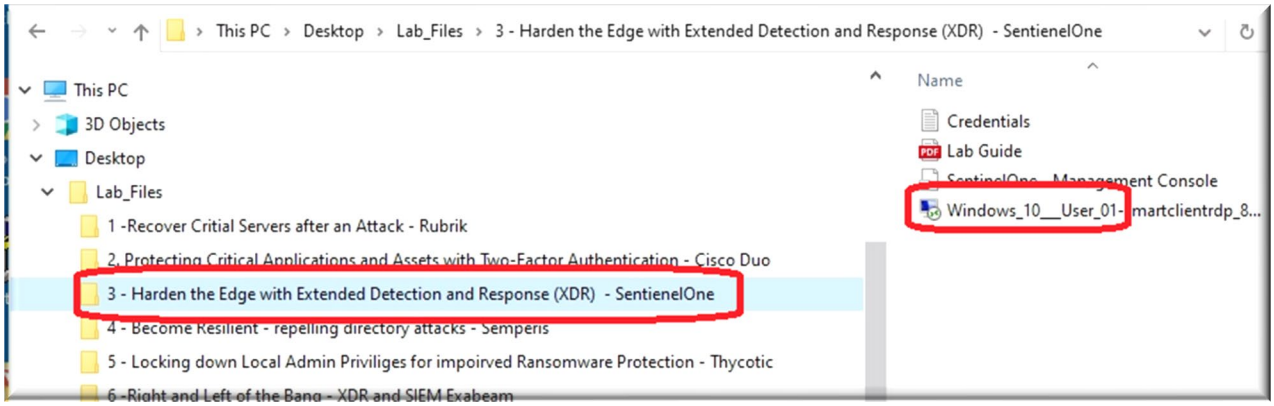
Now (if it is on your screen), click where it says MORE.

← This drills down to the type of event and where it occurred. Can we determine the differences (if any) that are in these events?

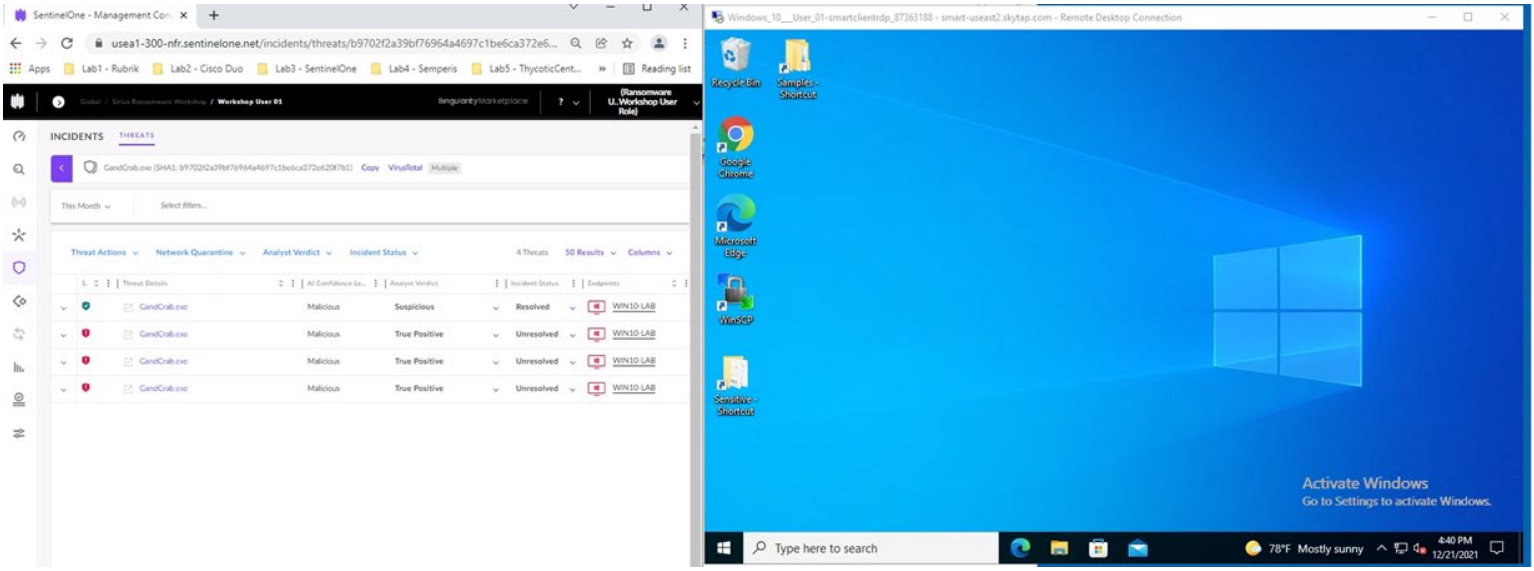
TASK 3: Login to the remote desktop virtual machines (RDP).

Navigate to the RDP (Remote Desktop Protocol) icon and double-click to launch. The username will be “Cathy Clark” (prefilled in) and the password is “Admin!23”

HINT: make the RDP window smaller and place the two windows side by side

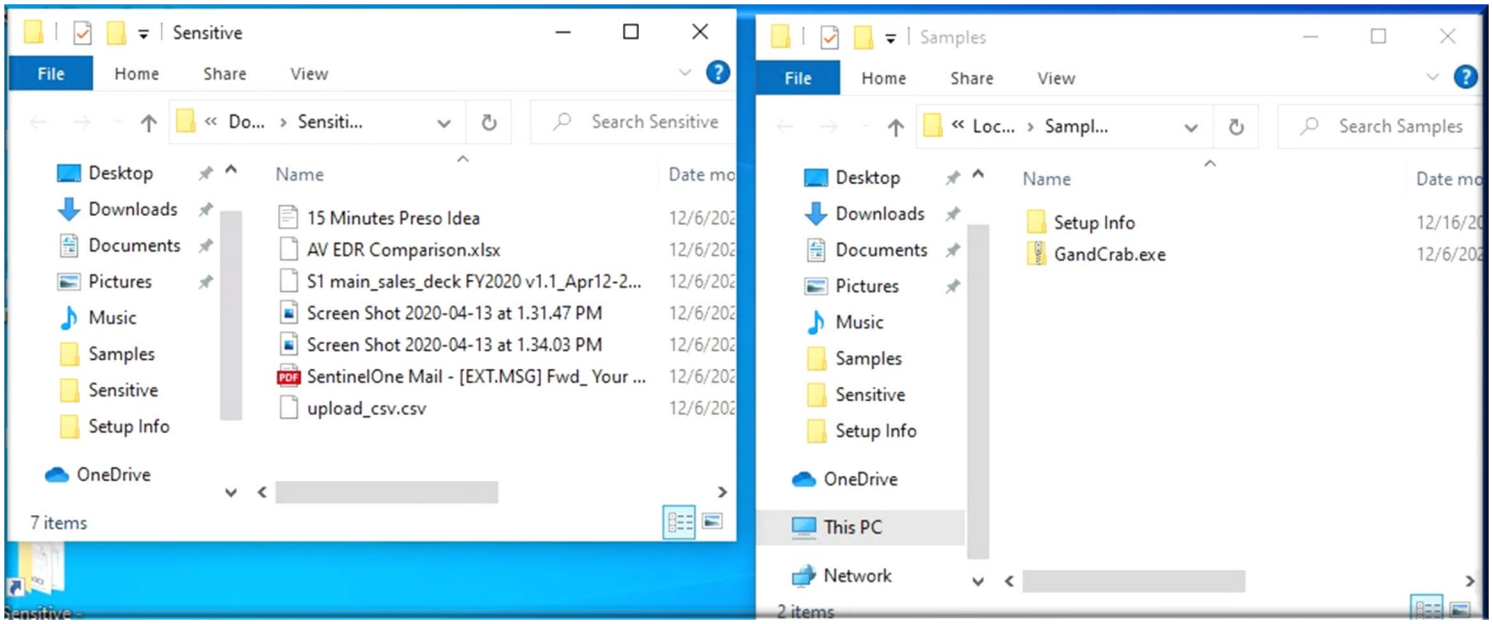


SHOWN BELOW ARE THE SENTINELONE CONSOLE and the RDP DESKTOP OPEN SIDE BY SIDE.



Task 4: Explore and setup the remote virtual desktop.

On the desktop (RDP connection), you should see two shortcuts to folders “Sensitive – Shortcut” and “Samples – Shortcut.” Open both folders and put side by side, if possible.



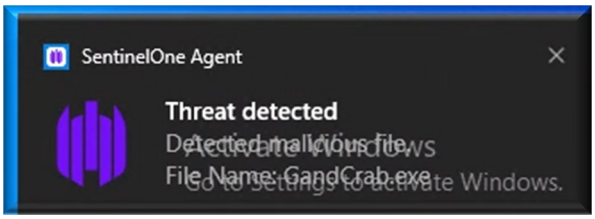
Above: Remote desktop connection showing the desktop and both folders open side by side.

In the folder where we have sensitive files, open a few of them to validate that they work. For example, opening the screenshot file should open a browser and display the images. You can also open a PDF file to review the airline receipt information from a recent trip or the TXT/CSV files. There are no Office apps on these remote virtual machines so we can’t open PowerPoint or Excel files, but we can validate that these files are good, not corrupt, and are in working order.

Task 5: Simulate a ransomware attack on this device.

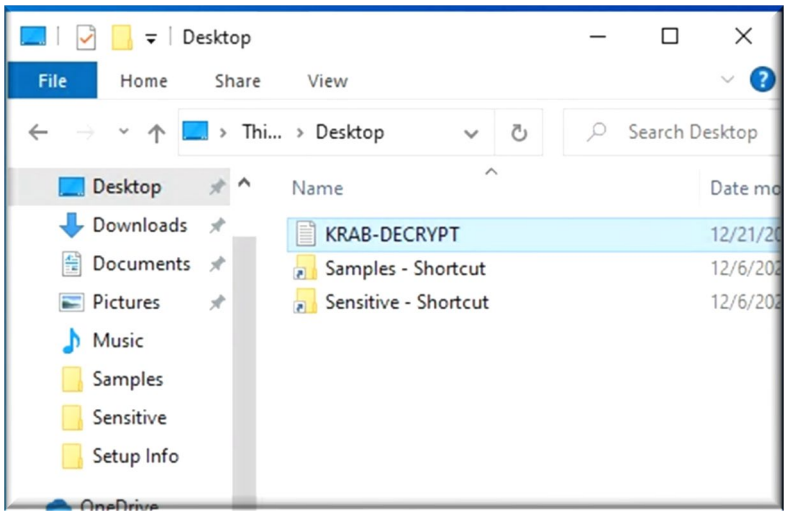
Move to the other open directory “Samples” and open a ZIP file containing ransomware. This could have been pulled down via e-mail, a website, a USB stick or various other methods. For the sake of this lab, we are knowingly opening this bad file, but remember that this could have been a successful phishing email with an attachment you thought was safe.

1. Open the zip file
2. Extract files to desktop
3. Execute the GandCrab.exe file



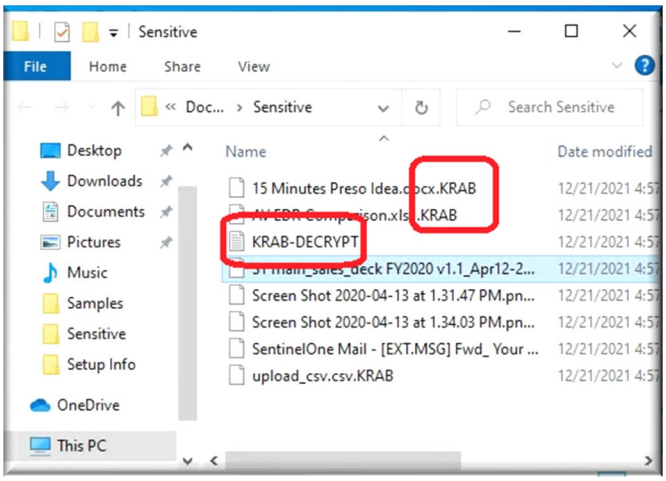
← Ignore SentinelOne pop ups.

SentinelOne flagged this activity, warned the user and sent an alert into the management console (we have the agent in monitor mode, otherwise is would have stopped this activity).



Look on the remote desktop and poke around the file system. Have you noticed anything strange?

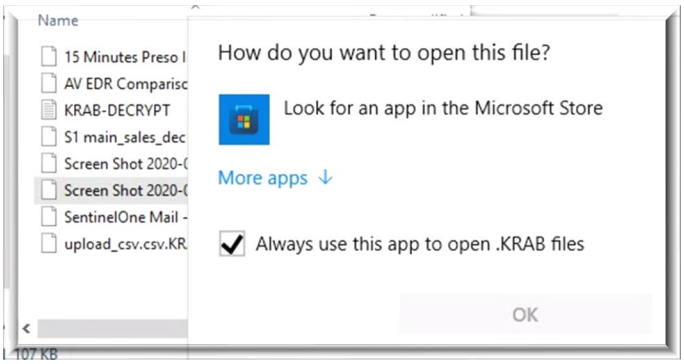
Open File Explorer, if not already open, and look around your desktop, folders and file system. Move to the Sensitive folder where your import documents are stored and try to open some of the files that you had opened before.



What do you notice?

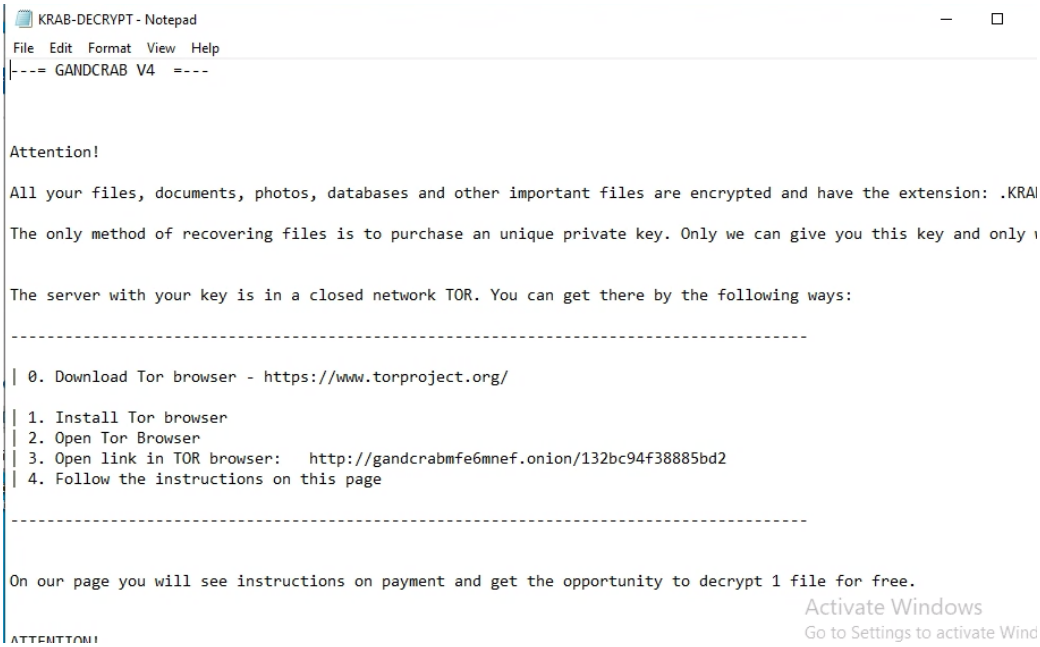
When ransomware strikes it is intended to hit hard and fast. Your system and terabytes of information can be lost within minutes. In this intentional infection, only a single machine is impacted as an example, but it shows how quickly it can happen.

Task 6: Try to open and use a sensitive file on the remote desktop.

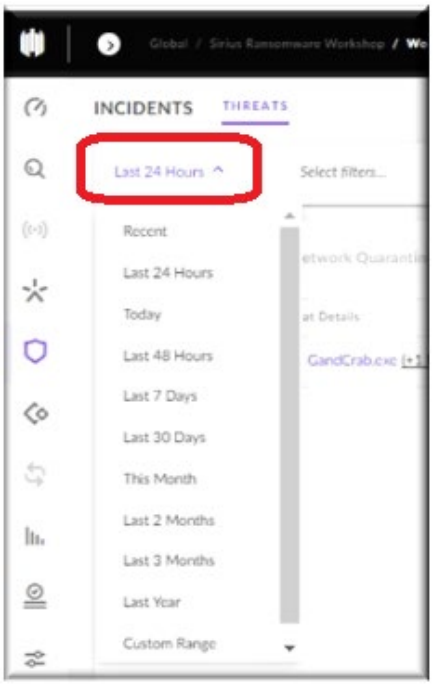


DOH! Our files have been encrypted and we can't open them.

Notice the ransomware message as well:



← You're hosed!!!!

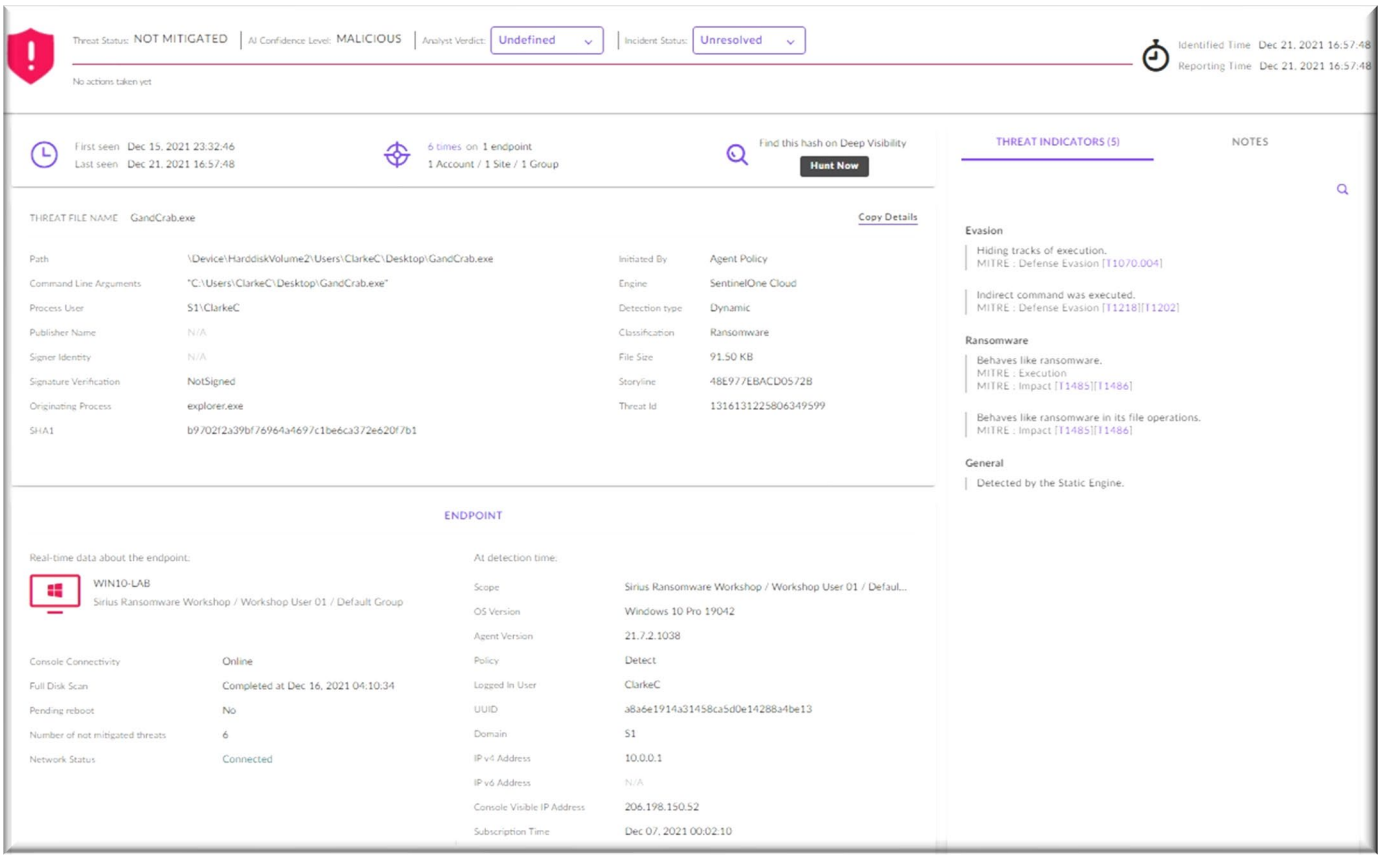


Task 7: Review in the console.

Let's go back to the console. Do you see more events now under Incident when you change the timeframe to last 24 hrs.?

You should see at least two different alerts from today about this incident. Can you determine what the difference is between the two events?

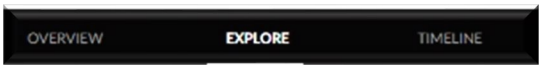
Let's pick the last event and drill into it, by clicking on the incident name.



Take a moment to look at the information presented. Notice or see if you can find the flowing information:

1. MITRE ATTACK framework reference *(hint: right click and select "Open in New Tab" when you find it)*
2. What device or person was logged in when this happened?
3. How many times has this event (or similar) happened?
4. Where was this incident noticed— what engine?
5. Static or dynamic?

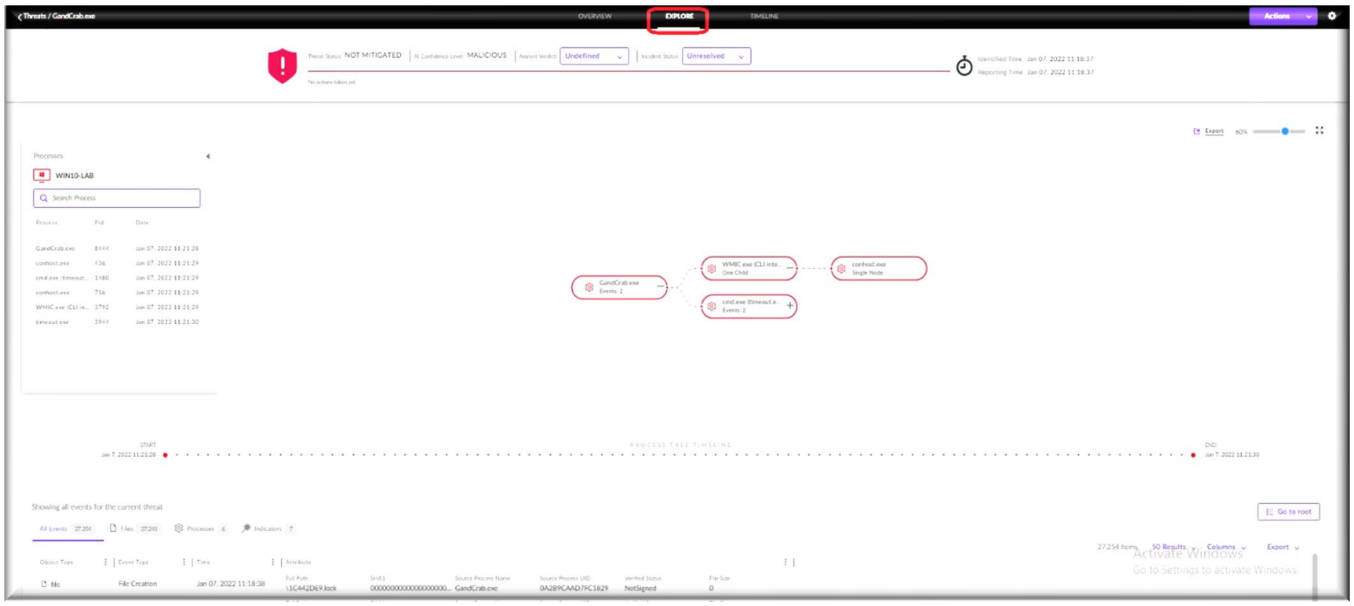
Up along the top of this incident, we have a few different TOP level menus:

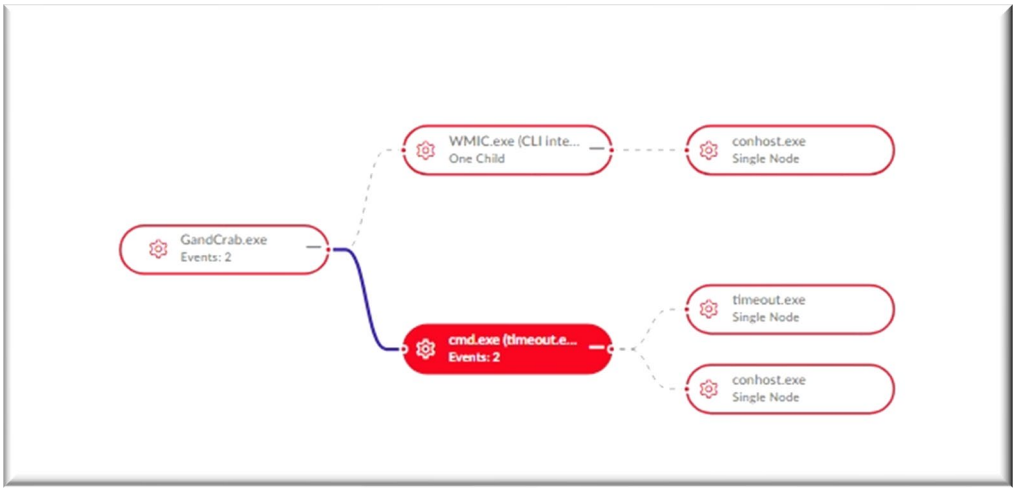


Overview / Explore / Timeline

Explore

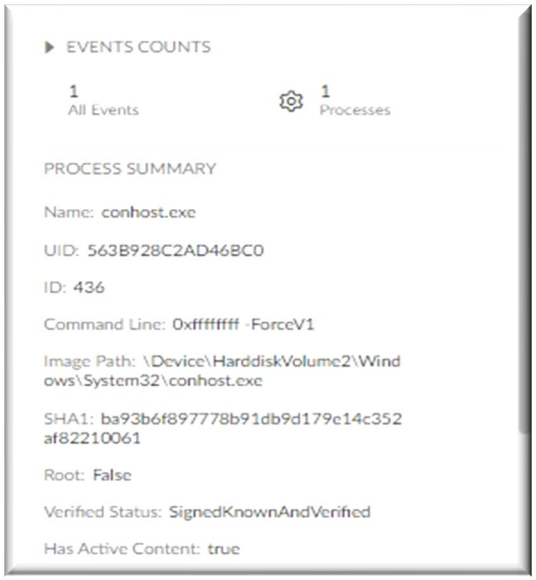
Look around and find the VISUAL representation of this event.



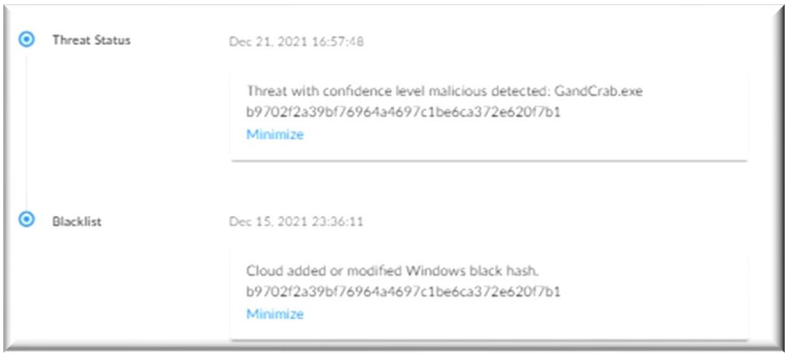


← Clicking on areas of the flow chart will focus the rest of the screen area on the details contained at that juncture. The other aspects of the screen, bottom half, process tree timeline and the far-right summary.

Summary Windows (right) -->



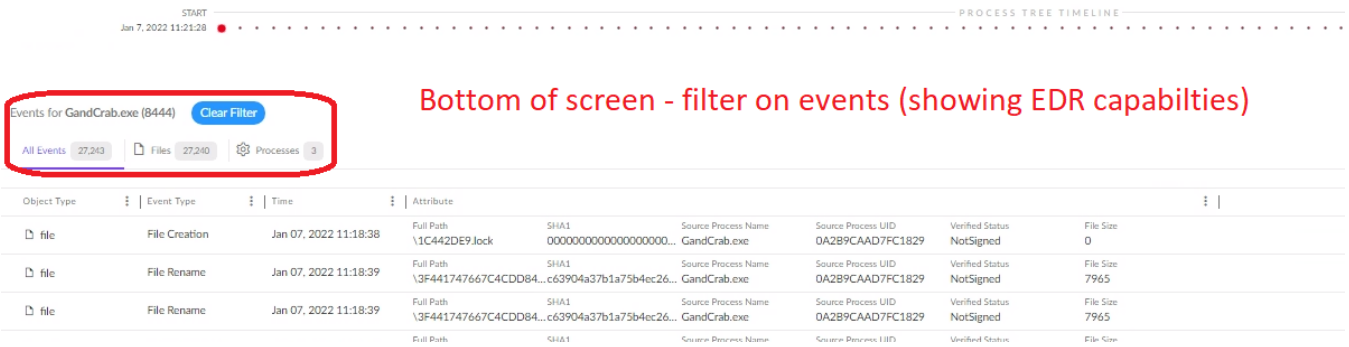
Below shows the timeline as you click along the visual above.



Timeline

Not incredibly interesting for this particular event, but notice that SentinelOne detected this as malicious and immediately placed it on the blacklist—hence protecting other devices.

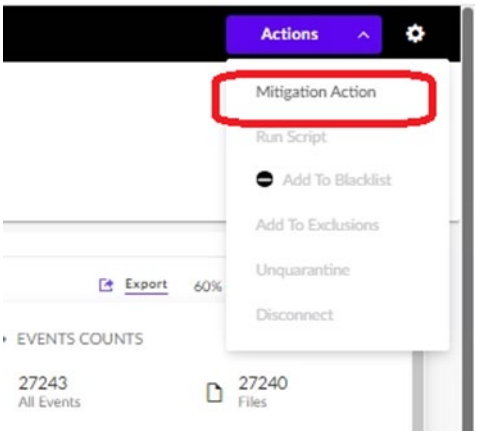
Task 8: Filter on events (bottom) of the visual representation.



Notice that SentinelOne captures everything that happened on the endpoint (EDR). Notice how much file activity occurred during this event (click on files to look at only file activity). What was the type of file activity that happened? Are these consistent with ransomware?

Change the focus to “Processes” to view the process started by the attack.

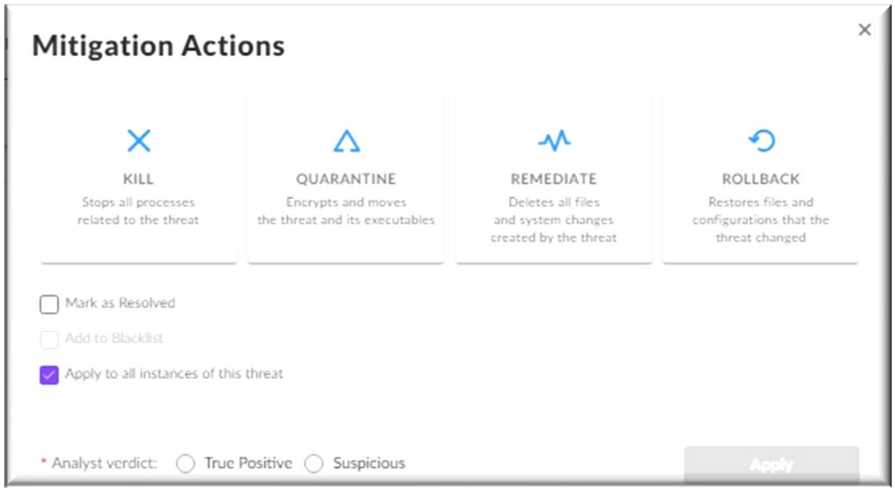
This allows us to quickly understand how ransomware behaves. Notice the last process that the attack attempted to do: “Shadow Copy Delete.” Most ransomware will attempt to disable and remove the Shadow Copy (Windows on disk backup) of your devices to prevent what SentinelOne can do next, which is to remediate and completely restore the endpoint so you don’t have to pay the ransom. SentinelOne does this because the agent, even in monitor-only mode, will intercept at a kernel level all calls to the Shadow Copy, preventing unwanted commands.



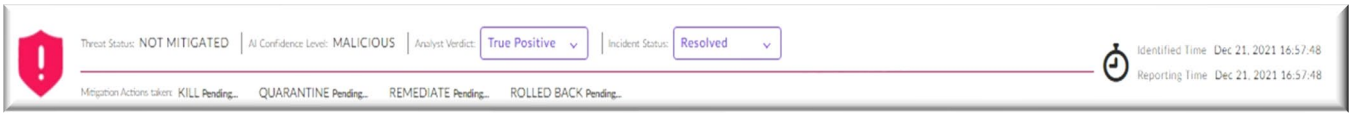
Upper Right of the screen, pull-down menu for actions select the “Mitigation Actions” from the menu

Notice that as you move from left to right, each of the steps will also execute the step(s) to the left. In this task, we are going to select “Rollback” on the far right, which will highlight all of the steps to the left and execute them, if they have not run already.

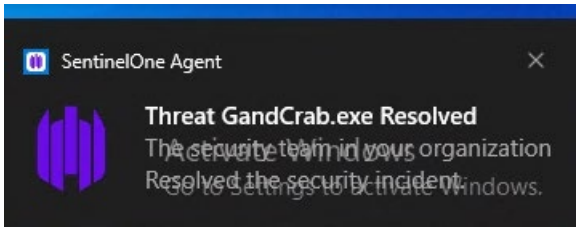
Lastly, you do need to have the “*Analyst*” verdict, in this case we know this event was a **True Positive** and click Apply

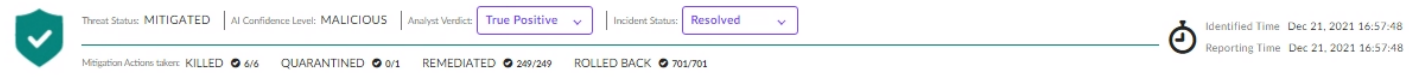


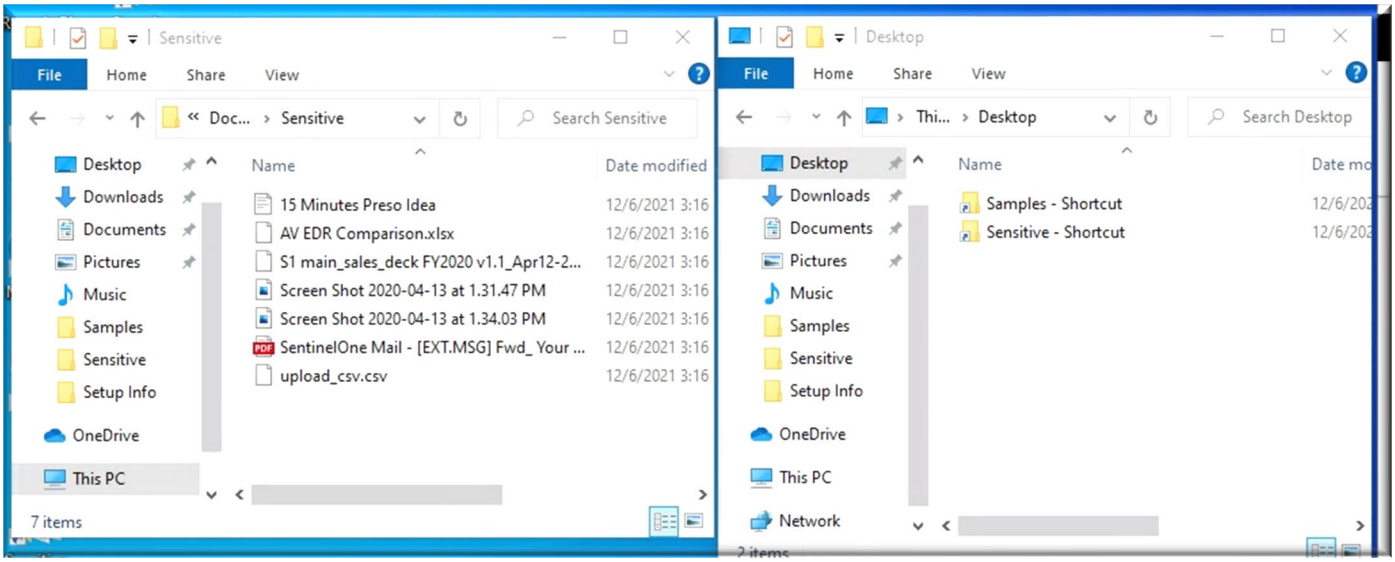
Notice the top the screen (below) showing the real time status of your action



Let's wait a few moments as SentinelOne performs these tasks and updates the status to complete. In a real-world attack, we would have hundreds if not thousands of devices that were affected and having SentinelOne perform these actions on ALL affected endpoints at the same time is an amazing capability.







Open some of the files. Validate that they are back to normal and that the user is now unaffected.

Summary –

SentinelOne allowed us to:

- Detect the issue
- Allowed us to VISUALIZE this, capture all important information/data
- Analysis across multiple devices
- Add to blacklist to further protect other devices
- Remediate the encryption and put the device and user back to work.