Security Research

Putting Things in Context | Timelining Threat Campaigns

Tom Hegel / May 11, 2022

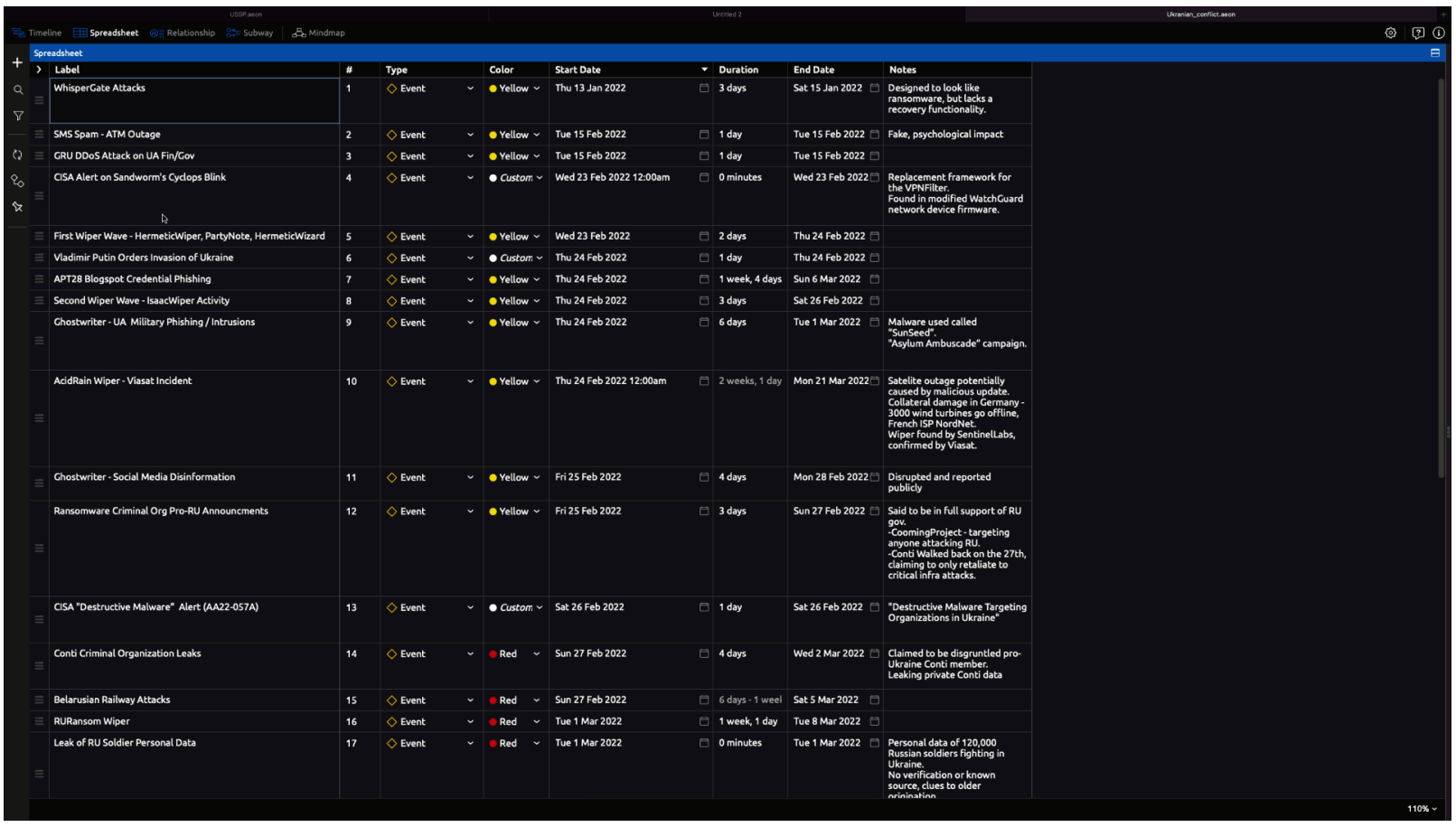
Like many in our field, I often have a desire to timeline a threat or mind map threat activity to better understand evolving campaigns, track new unknown activity, and generally keep up with the ever-changing threat landscape. Timelining threat campaigns is incredibly useful for many reasons. For one, we are often faced with complex incidents that need a form of documentation to enable the identification of new context. Being able to see how events relate to one another is powerful because it allows a researcher to organize complex threat activity and highlight context an actor cannot easily fabricate, even when considering specific misdirection techniques like file timestomping.

In this post, I'm going to walk through some examples of how I use Aeon Timeline. I'll also provide a custom threat research-themed template for your own use. Additionally, this blog contains the timeline file we made while tracking the threat activity related to the invasion of Ukraine. I hope this will encourage other security researchers to make use of timelines as a foundation to further their own research or for historical reference of related events.

What is Aeon Timeline Software?

I've found Aeon increasingly useful while researching threat activity, and I would highly recommend it for security practitioners. For some context, Aeon Timeline is an interactive timeline tool used for a variety of industries, such as legal, creative writing, and education.

While our use in security research is rather unique, many of its features can be used for our purposes. Since Aeon currently does not come with a preloaded configuration/template for security research projects, I would like to use this blog to share our template, which you can now download and import.



Label	#	Type	Color	Start Date	Duration	End Date	Notes
WhisperGate Attacks	1	Event	Yellow	Thu 13 Jan 2022	3 days	Sat 15 Jan 2022	Designed to look like ransomware, but lacks a recovery functionality.
SMS Spam - ATM Outage	2	Event	Yellow	Tue 15 Feb 2022	1 day	Tue 15 Feb 2022	Fake, psychological impact
GRU DDoS Attack on UA Fin/Gov	3	Event	Yellow	Tue 15 Feb 2022	1 day	Tue 15 Feb 2022	
CISA Alert on Sandworm's Cyclops Blink	4	Event	Custom	Wed 23 Feb 2022 12:00am	0 minutes	Wed 23 Feb 2022	Replacement framework for the VPNFilter. Found in modified WatchGuard network device firmware.
First Wiper Wave - HermeticWiper, PartyNote, HermeticWizard	5	Event	Yellow	Wed 23 Feb 2022	2 days	Thu 24 Feb 2022	
Vladimir Putin Orders Invasion of Ukraine	6	Event	Custom	Thu 24 Feb 2022	1 day	Thu 24 Feb 2022	
APT28 Blogspot Credential Phishing	7	Event	Yellow	Thu 24 Feb 2022	1 week, 4 days	Sun 6 Mar 2022	
Second Wiper Wave - IsaacWiper Activity	8	Event	Yellow	Thu 24 Feb 2022	3 days	Sat 26 Feb 2022	
Ghostwriter - UA Military Phishing / Intrusions	9	Event	Yellow	Thu 24 Feb 2022	6 days	Tue 1 Mar 2022	Malware used called "SunSeed". "Asylum Ambuscade" campaign.
AcidRain Wiper - Viasat Incident	10	Event	Yellow	Thu 24 Feb 2022 12:00am	2 weeks, 1 day	Mon 21 Mar 2022	Satelite outage potentially caused by malicious update. Collateral damage in Germany - 3000 wind turbines go offline, French ISP NordNet. Wiper found by SentinelLabs, confirmed by Viasat.
Ghostwriter - Social Media Disinformation	11	Event	Yellow	Fri 25 Feb 2022	4 days	Mon 28 Feb 2022	Disrupted and reported publicly
Ransomware Criminal Org Pro-RU Announcments	12	Event	Yellow	Fri 25 Feb 2022	3 days	Sun 27 Feb 2022	Said to be in full support of RU gov. -CoomingProject - targeting anyone attacking RU. -Conti Walked back on the 27th, claiming to only retaliate to critical infra attacks.
CISA "Destructive Malware" Alert (AA22-057A)	13	Event	Custom	Sat 26 Feb 2022	1 day	Sat 26 Feb 2022	"Destructive Malware Targeting Organizations in Ukraine"
Conti Criminal Organization Leaks	14	Event	Red	Sun 27 Feb 2022	4 days	Wed 2 Mar 2022	Claimed to be disgruntled pro-Ukraine Conti member. Leaking private Conti data
Belarusian Railway Attacks	15	Event	Red	Sun 27 Feb 2022	6 days - 1 week	Sat 5 Mar 2022	
RURansom Wiper	16	Event	Red	Tue 1 Mar 2022	1 week, 1 day	Tue 8 Mar 2022	
Leak of RU Soldier Personal Data	17	Event	Red	Tue 1 Mar 2022	0 minutes	Tue 1 Mar 2022	Personal data of 120,000 Russian soldiers fighting in Ukraine. No verification or known source, clues to older origination

To get hands-on experience, here are two ideas of what you can do with the Ukraine timeline shared here:

- Label events as either cyber or kinetic, then begin documenting the kinetic events of the war. How do the events now line up, and do you see any correlation of the two?
- Cluster the activity by threat groups

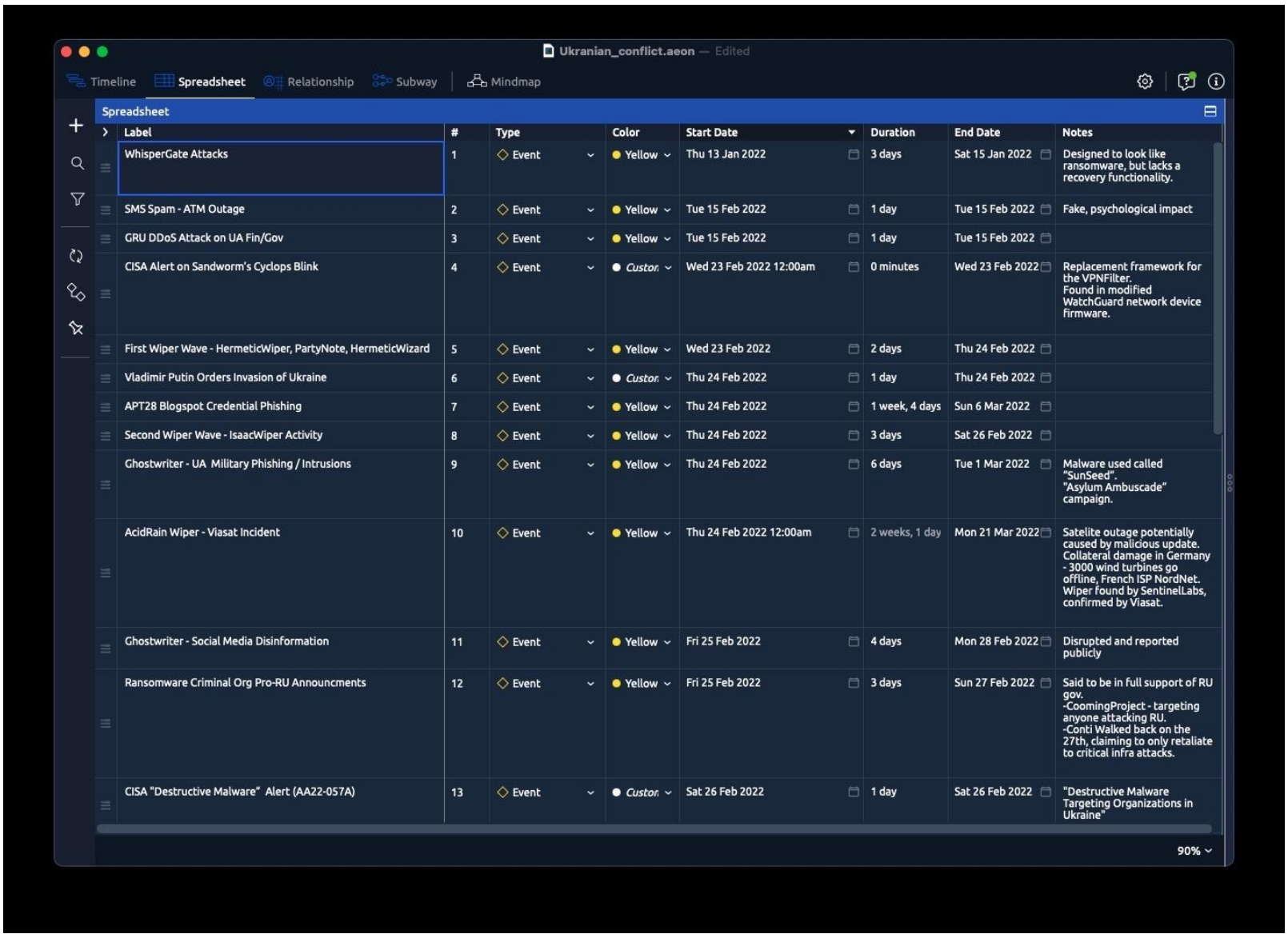
Aeon is superb for these kinds of uses and many others, although I would recommend against using it as a form of TIP (Threat Intelligence platform) or for generally collecting and storing intelligence long term. I recommend its use during an initial investigation's learning phase, and once complete or at a level of confidence, storing the data (as appropriate) in a central platform like the Vertex Project's Synapse. This would ensure proper data retention and long-term value. However, the tool is rather adaptable so it's ultimately your choice on how it can be used.

Create and Explore a Timeline

Let's take a look at some basic timeline creating workflows. In order to use the timeline, we need data, which in the case of Aeon can best be viewed in the "Spreadsheet" tab at the top. Data stored in the spreadsheet can be heavily customized, including their properties.

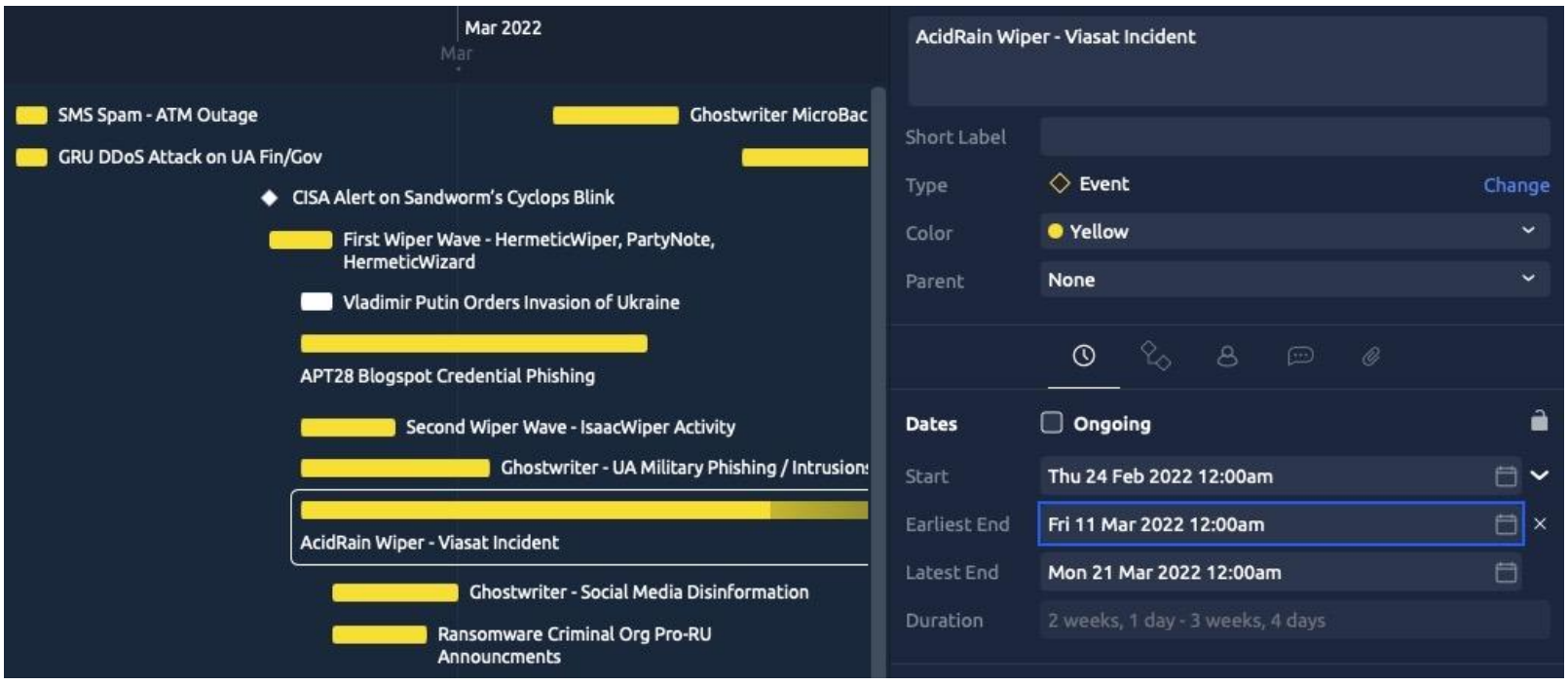
For this example, we'll use the file shared related to the cyber domain events centered around the invasion of Ukraine. Also note, this example is heavily based on events rather than individual IOCs which we would make use of on a deeper level or in a mind map depending on your need.

My overall objective of this timeline was to grasp what happened and when, considering the flood of activity at the time was difficult to make sense of. The data used in this timeline is generally based on OSINT, which we can expect will change as we learn more about the events referenced, which is why having an easy to use timeline works so well.



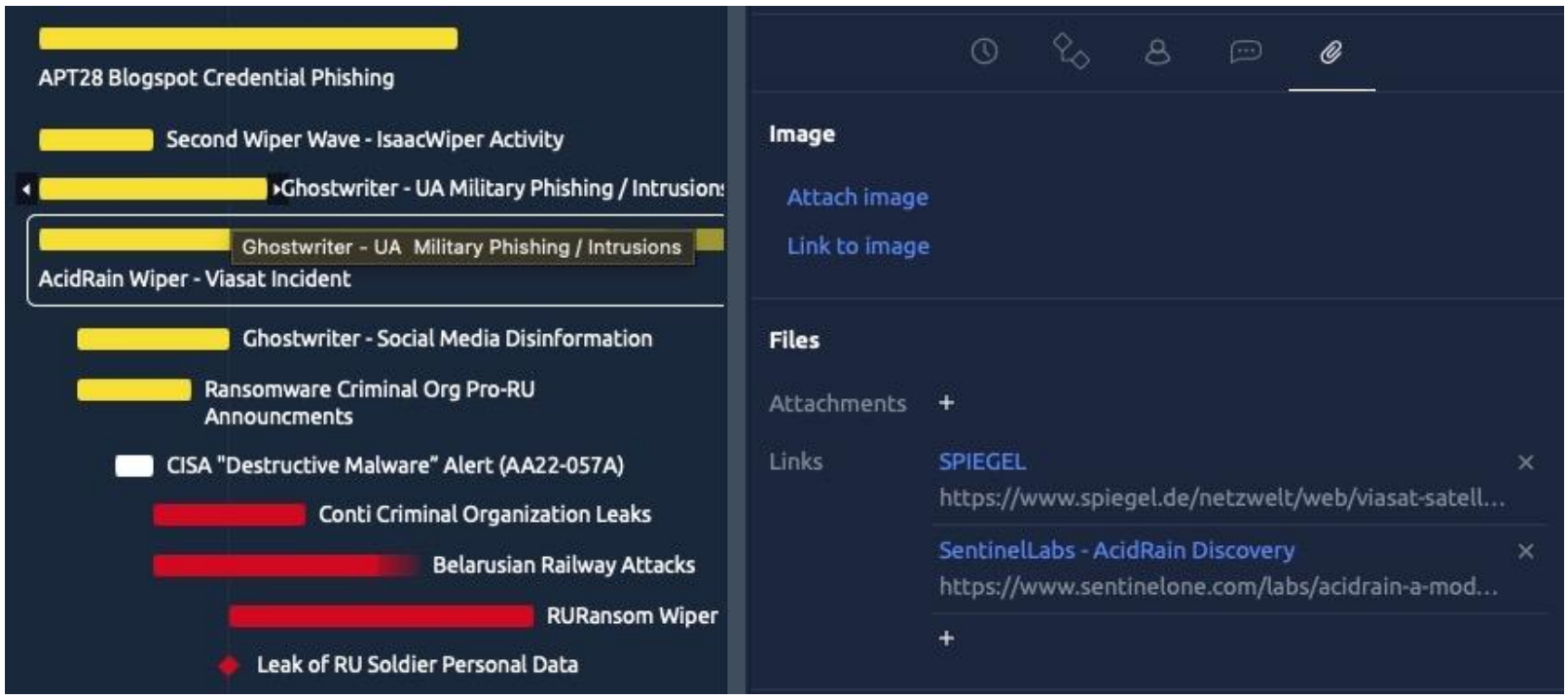
Spreadsheet Data to Form Timeline

Here is a section of the data itself, which as you can see, contains labels, notes and times. I made use of colors to theme pro-Russian vs pro-Ukrainian events to make use of when looking at it from a higher level. In many of these cases, my working idea is to note the start and end dates, knowing that they are again, based on OSINT, but likely limited based on perspective of the source. You can visually indicate that on the timeline by opening the event to see its included properties and using the earliest/latest dates.



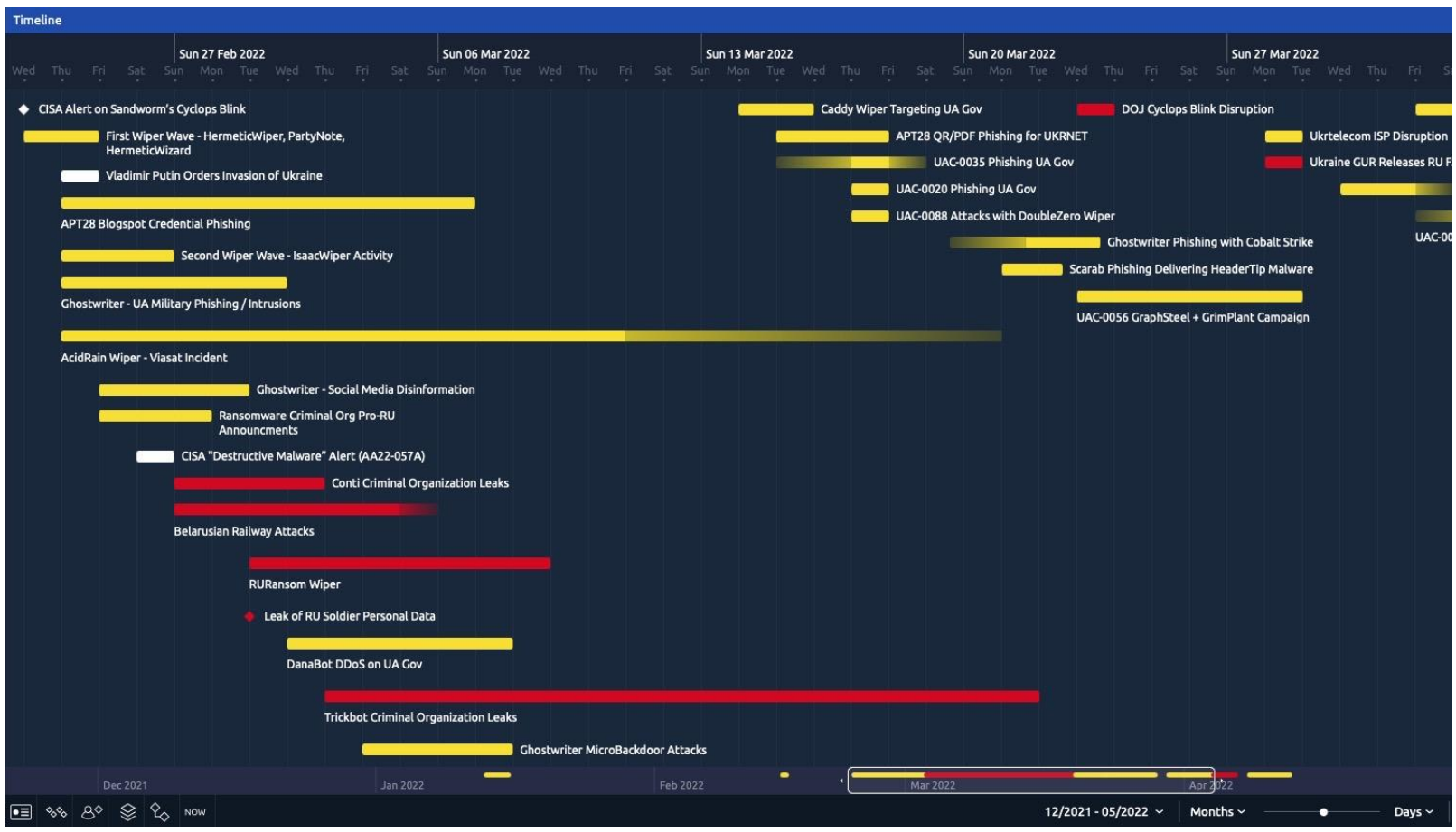
AcidRain Event Example of Dates

Additionally, in the properties I often make use of Notes and links/images. The timeline we're looking at has many references to each event for your own analysis.



AcidRain Event Example of Links

After placing dates/times on our events, we can begin reviewing them in the timeline tab at the top of the application. As you can see below, we have quite an interesting timeline of events giving perspective into the quantity of known/public events on this topic, while also giving us the references to each.

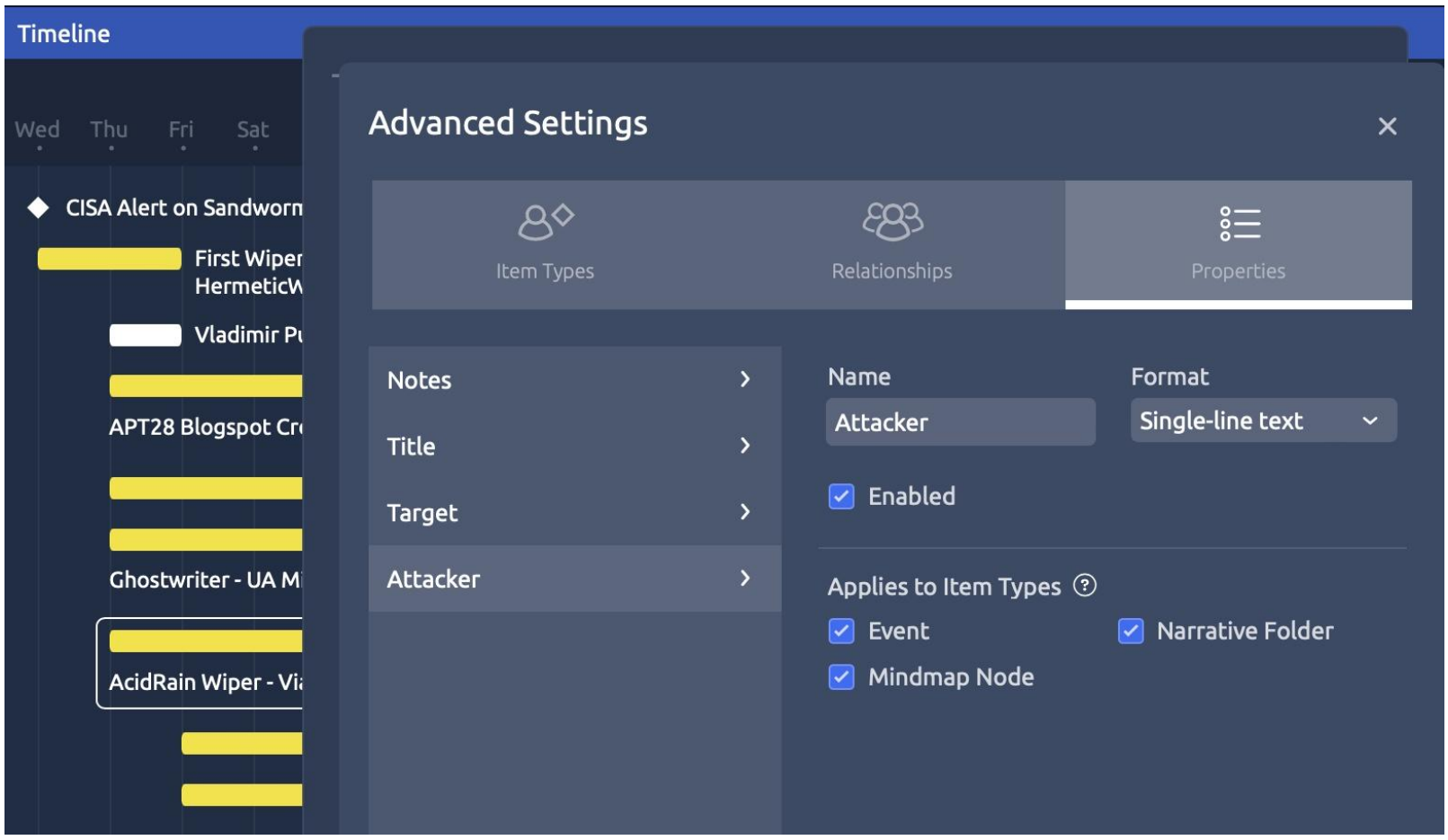


Timeline of Ukraine-centric cyber activity

I recommend exploring the bottom right and left options to best display the information to your liking. Zooming in for specific dates and out for high level overviews (like above). This above timeline expands to a view of months and indicates precise days with vertical lines. However, if you are using a timeline for something like an intrusion analysis, you will likely find value in using a deeper precision like minutes.

Personally, my workflow for the Ukraine events was kept rather manual because of my desire to review, understand, and expand each event when possible. However, as you begin using the application you will quickly find the option to bulk import data, which may now feel similar to something like Maltego.

Additionally, when it comes to customizing properties, it all depends on what you could find useful. For example, if I'm particularly interested in tracking the target organization or attacker by event, simply add it as a property of the data. To do this, click the top right ⚙ (Settings), Data Types > Edit > Properties.



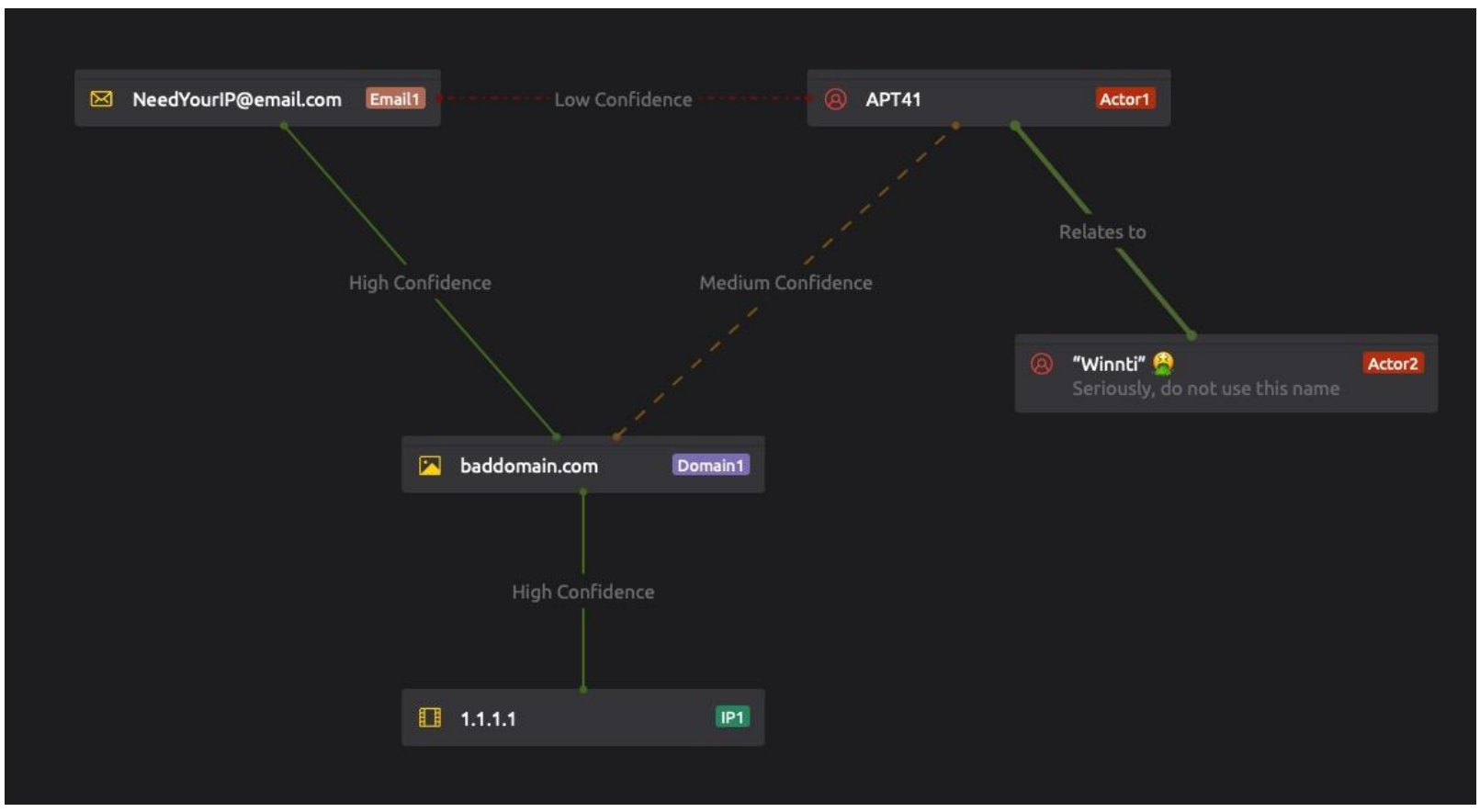
Adding Target and Attacker properties

Mastering The Mind Map

On a much different level, one other great area of the product I make use of is the mind map. My use of a mind map is of course more related to the discovery of relationships rather than time of events. Generally speaking, the mind map is my go-to for connecting the dots between the larger and more complex bits of threat activity. A mind map was instrumental in my research on ModifiedElephant.

The template shared in this blog post will be a great starting point for your own mind map use. To get started, open a new project using the template, then navigate to the top mind map section. Double-click in the empty map to add your first entity. Once multiple entities exist, you can connect the two by forming a line relationship. The entity types and relationships are built into our template, so you can customize to your liking.

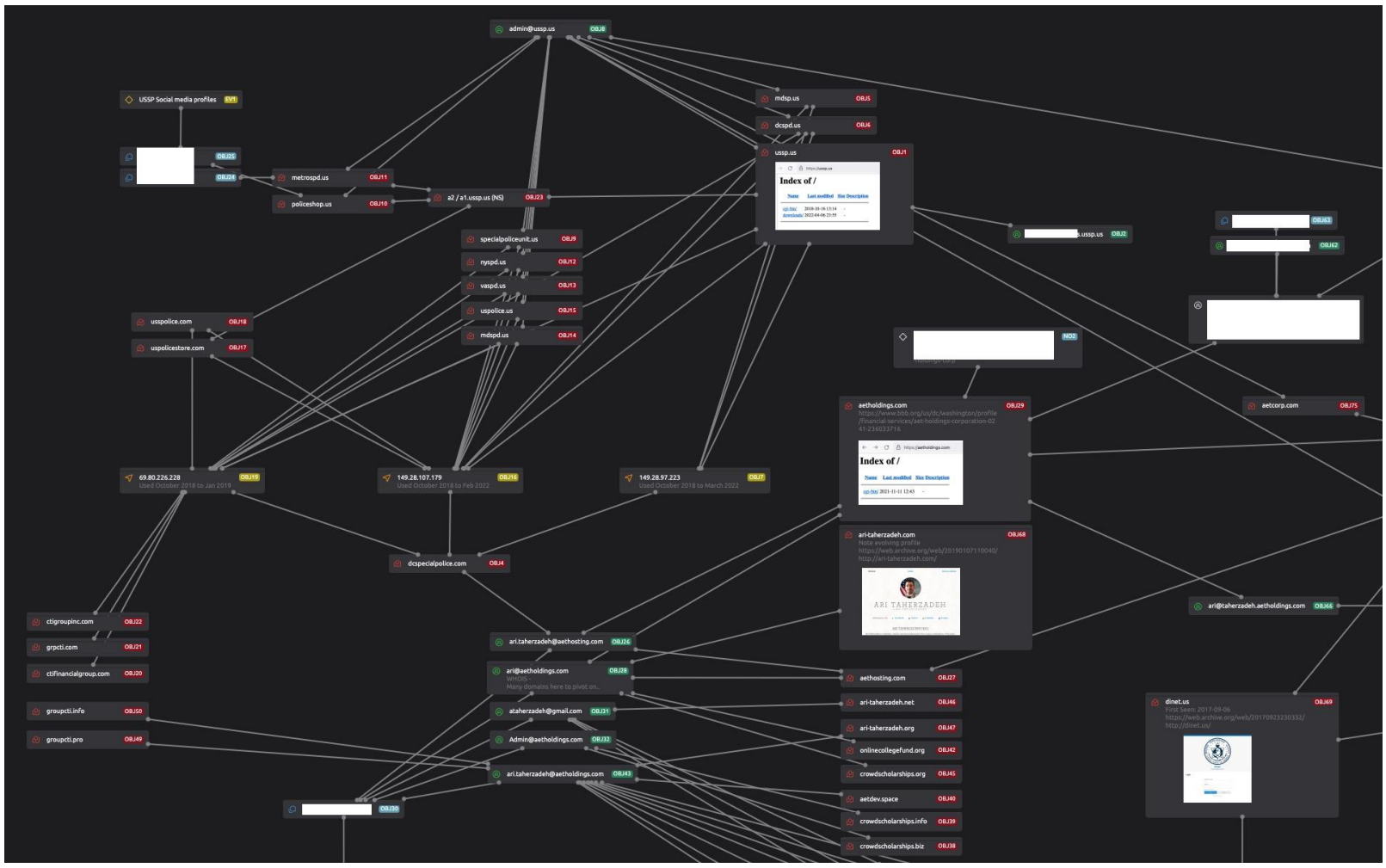
Here is a quick example of how one could use the mind map to quickly map out some activity while also noting potential assessments of confidence. Note that we have a domain IOC which is related with high confidence to an IP and email. Those then further relate to the infamous APT41.



Mind Map example, clean and organized

To modify all the data types (IOCs in this case), Relationships (confidence levels), or properties of the data, again navigate to the advanced settings: ⚙ > Data Types > Edit.

It's also worth noting that a mind map does not need to be highly organized and clean. Sometimes if I'm moving fast, a mind map just to keep track of my findings is often good enough to avoid forgetting something. However, if you plan on maintaining the map over time rather than a quick project, I recommend avoiding such methods or you could end up with something less than helpful like the one below.

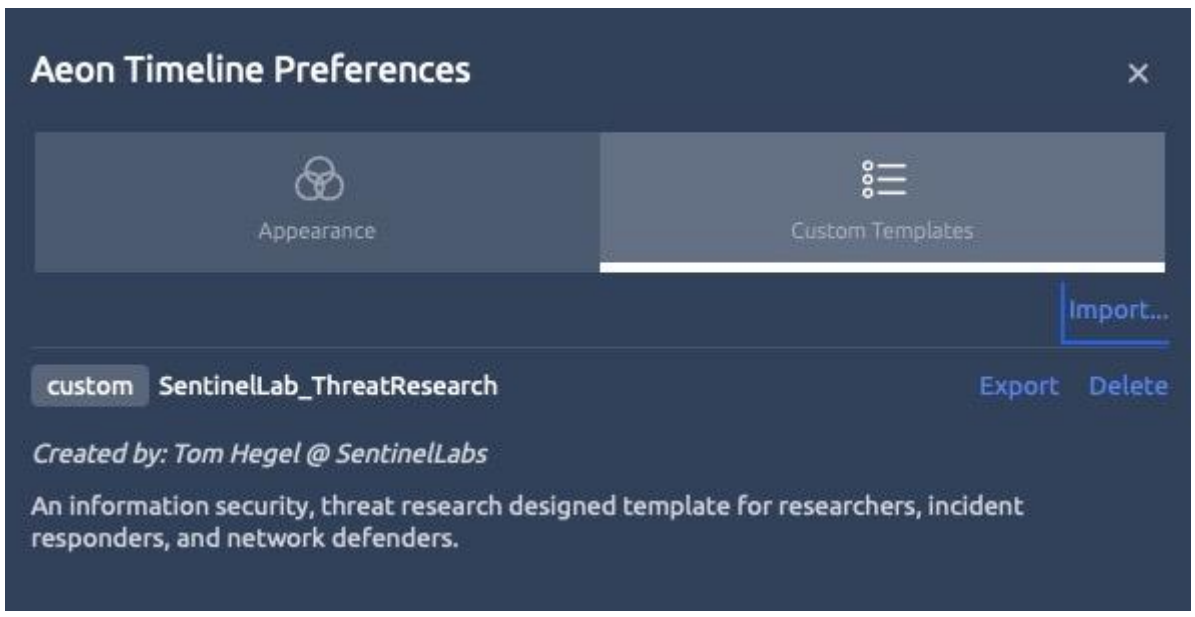


Messy mind map — does it help or hinder?

Custom Template — Download and Open

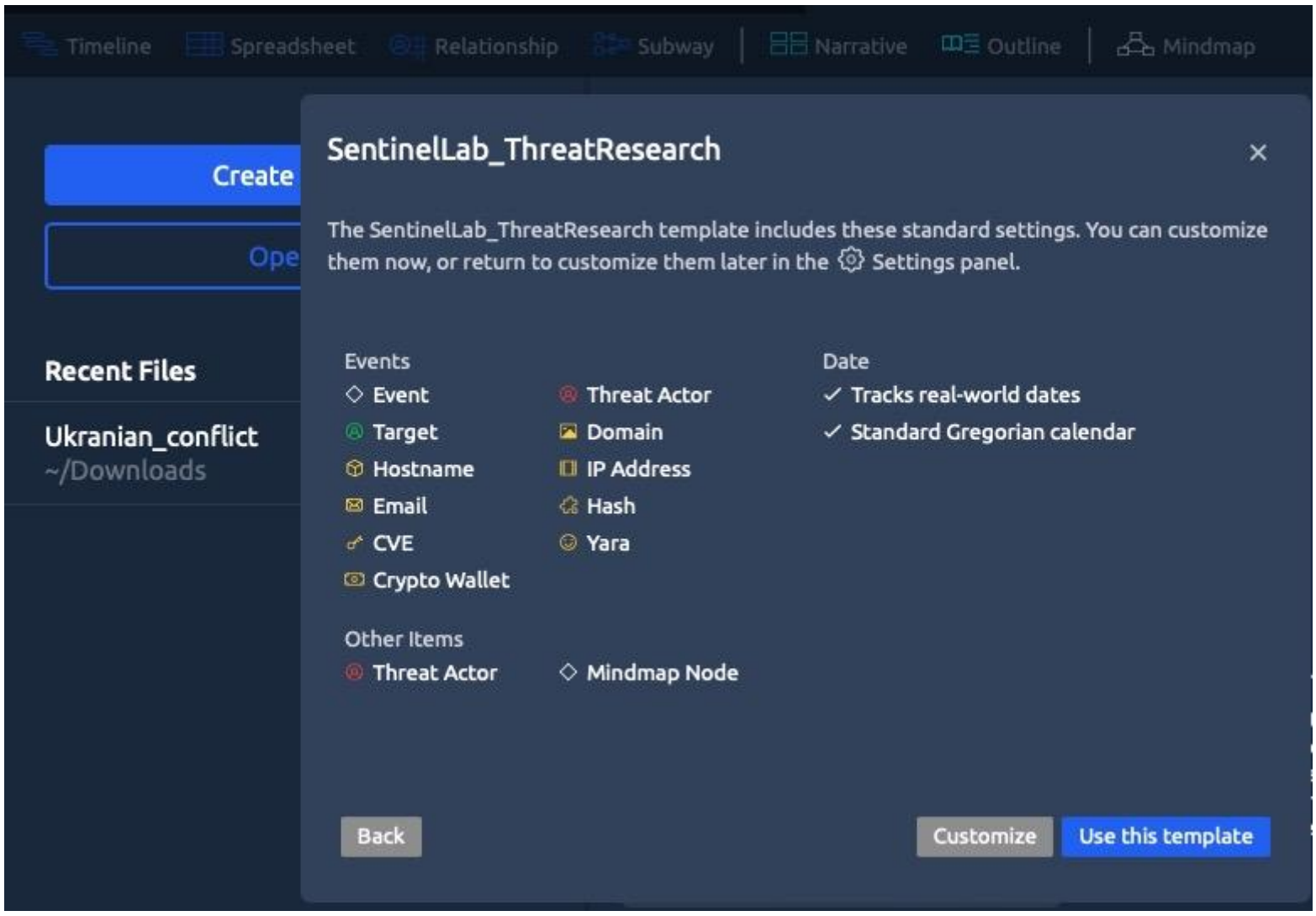
Below you will find an example timeline and mind map, but I also highly recommend exploring the official training material on the Aeon website in order to understand more of the tools capabilities.

After installing Aeon, download our template file and save it locally. With Aeon running, navigate to the program preferences and select custom templates. Here is where you can import the SentinelLabs template you previously downloaded.



Import Aeon Template

On the main page of Aeon, select Create New > Custom, and you should see an entry for the template, which is preconfigured with common IOC types used in the practice of security research. The template is completely customizable to your personal needs, but the setup provided should be enough to get you started.



Template IOCs and Configuration

You are now ready to use the tool for some interesting threat research use cases.

Conclusion

Analysts, researchers, incident responders, and any other form of investigator can derive a lot of value from this tool. If you want to get started, download the template and the UA/RU timeline to explore the data.

The use of timelines in the researcher workflow is a powerful tool that can help enable the identification of new context. I hope the examples shared here may motivate others to adopt them as a useful addition to their toolkit and industry collaboration efforts.