EU ATT&CK Workshop Q&A: Day 1

Q. Will you have mapping for NIST 800-160 (Cyber Resilience)? Adam Pennington: We are currently working on a mapping to 800-53. We've gotten a few questions about 800-160, so it's on our radar, but we don't currently have any plans.

Q. Where can we find the agendas for both days of the workshop? https://www.attack-community.org/event

Q. Beta looks good! will this affect the current API? Adam Pennington: There are a few small changes to our STIX representation to let us represent the sub-technique relationship, but everything else is staying the same.

Q. What could be a good strategy in order to mature and evangelize Attack in Enterprises? Adam Pennington: Depending on where you're starting at, our Getting Started series (https://www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf) was intended to help in this space. Beyond that, probably the best collection of resources we have is at https://attack.mitre.org/resources/getting-started/ where we've collected quite a bit based on use case.

Q. Is it planned to expand / refine the mitigation area? Adam Pennington: We have ongoing work on mitigations for ATT&CK for Mobile and ATT&CK for ICS, and add to mitigations in ATT&CK for Enterprise as we receive contributions suggesting them.

Q. Is there any behind the scenes going on with traditional security vendors in mapping / aligning against ATT&CK and providing product specific mitigations? Adam Pennington: We talk with a ton of community members about how they're leveraging/mapping ATT&CK. Product-specific mitigations are probably not on the radar for us, as it becomes very hard to stay vendor neutral. Probably the closest we come is the work the ATT&CK Evaluations team has been doing (https://attackevals.mitre.org/)

Q. Can you elaborate on recent developments in YARA-L, how do you compare it with SIGMA? Florian Roth: It is not that easy to answer that question in a chat. I think that both standards are not that different, although it seems very different while looking at the complex (almost "script language"-like) conditions in YARA-L. I think the main reason not to adopt Sigma within Chronicle was to have full control of where it's heading and add the features that are needed to satisfy requirements within their platform without having to discuss it with the maintainers of an open source project. I completely understand that. If I were a Chronicle customer, I'd look further into YARA-L and leave Sigma aside for now. It's possible that we provide a YARA-L backend somewhen in the future.

If I weren't a Chronicle customer, I'd expect that YARA-L gets optimized for their Backstory platform. The complexity that comes with this optimization and alignment most likely makes it difficult to adopt the standard in other platforms. I'd always prefer an open standard without influences by a certain vendor.

Q. Regarding Sigma most of my rules use some big whitelisting, blacklisting or reference set (Qradar) how could you handle that in the sigma format? Florian Roth: Whitelisting / blacklisting can be done within the rules. Placeholders for what QRadar calls reference sets are on the roadmap.

Q. Where is the relation between SIGMA and MITRE ATT&CK Framework? Florian Roth: Sigma rules contain MITRE ATT&CK tags. A triggered Sigma rule in your SIEM can immediately lead you to the corresponding technique.

Q. Is it okay if the cooking link is posted here? Infosecwelldone.com

Q. Do you plan to extend data dictionaries towards ICS as well? Roberto Rodriguez: Yes, we will extend the project to more platforms. We need help on covering more platforms of course. It would be awesome to learn more about ICS and see how data can be collected.

Q. Would you please advise if there is valuable resource to look at in regards threat hunting queries that based on "Advance Hunting WDATP"? Regarding other APTs, will they be covered as well? Roberto Rodriguez Thank you for the feedback :) MDATP will be available to be exported/streamed directly to tools like Azure Sentinel so I assume it will be possible to export that data in a lab environment. For now, you can look at all the queries created in here (https://github.com/OTRF/detection-hackathon-apt29/projects) for some ideas where MDATP can hel (i.e. Registry, Process, etc).

Q. What was Roberto's slack channel? Roberto Rodriguez: https://launchpass.com/threathunting

Q. Will you be expanding the current threat hunters use cases on the threathunters forge? Roberto Rodriguez: Would you mind providing more context? Do you mean extending the APT29 detections to targeted small detections? Hunters-Forge is the Public GitHub repo

Q. Andrii Bezverkhyi, would you please advise what is the best method to reach out to you if we have question? Andrii Bezverkhyi: Thank you. Twitter @andriinb is best way, feedback is most welcome.

Q. What will be the approximate cost of the infra that will be spawned? Patrick Bareiss: This depends on the EC2 instance type which you choose, and which can be changed to a smaller one. We not yet did some calculations but as we already got this question multiple times, we will do some estimations.

Q. How would you compare the Splunk Attack Range vs. Detection Lab? Patrick Bareiss: In my opinion the Detection Lab is a great project for a lab environment whereby our main goal was to use the Attack range in a CI pipeline and do automated detection testing.

Q. Do you have plans to support GCP or Azure? Also - do you know the cost (per hour, per day or whatever) of the lab in AWS? Patrick Bareiss: You can change the type of EC2 instance which you want to use and therefore reduced the cost if needed. We didn’t do some estimations, but we will do. In the future we also want to support Azure and GCP.

Q. Does Splunk instances (ES/Phantom) that are a part of attack range deployed infrastructure require licenses or connection to existing license master or they shipped with a trial license? We use terraform in conjunction with vCenter. **Any plans for developing attack range integration for that as well? If not, will it be useful if we create one and share with community? Patrick Bareiss:** The Splunk instance is shipped with a trial license. Phantom would need a registration but also have a trial license. For an ES trial you would need to contact your Splunk sales. We not yet have a look to host in it vCenter but we are open for pull request and working together with you on that topic.

Q. I would like to read more about sigma, where is good source of valuable documentation? Andrii Bezverkhyi https://github.com/Neo23x0/sigma

Q. How do you measures criticality level and reliability level for supercharging use cases in threat modelling? Do you pull it outsource or you have those measurements built by yourself? Ion Santotomas: Criticality can be measured with an impact matrix (probability of occurrence + impact of occurrence). For the reliability level you can use DeTTect to assess your detection quality. They have a scoring sheet that I found very useful.

Q. I’m not a big fan of so called “closed standards”. I am curious about your views on the benefits of conditionals in detection rule creation? Also, is there any plans to add this kind of feature to SIGMA? Florian Roth: Yes, conditionals are on our to-do list. Personally, I am not a big fan of them, but I see the value in them. YARA, which I use daily and for years, also has this option and I try to avoid it wherever I can and rather accept some redundancy to keep complexity of the rule set minimal. Whenever you have to resolve references between rules before or during processing a rule set issues arise (e.g. when you apply filters). I think we will introduce it in an adequate and use case focused form.

Q. Is MISP being used as a "use-case bucket"? James Morrin: We export a copy of the metadata around our UCs from our SIEM to MISP - and generate a MISP galaxy from the data. This allows us to then tag up reports/ideas

where there is a relevant UC. The UCs themselves however our stored in the SIEM. Hope this helps.

Q. What kind of TIP platform are you using for structuring intelligence data? James Morrin: We are using MISP for our intelligence platform, and the include MITRE galaxies for structuring. We've then done some customization using the tags and MISP objects to help our workflow and structuring.

Q. You mentioned a great resource for listing data sources, sub-data sources, data object, relationship, Event ID, et c. - what project is this related to? I saw a link to a google Spreadsheet, but wasn’t able to copy it down to review. Scott McKean: Checkout the Threat Hunter's Playbook project here: https://github.com/hunters-forge/ThreatHunter-Playbook Or here for the readable notebook: https://threathunterplaybook.com/pre-hunt/data_modeling.html Link to the spreadsheet here: https://docs.google.com/spreadsheets/d/1ow7YRDEDJs67kcKMZZ66_5z1ipJry9QrsDQkjQvizJM/edit#gid=0

Q. How possible it is to include regex in sigma to have a more accurate string detection? Thomas Patzke: You can do this with the value modifier "re", e.g.: CommandLine|re: '.*foo.*bar' Docs: https://github.com/Neo23x0/sigma/wiki/Specification#value-modifiers Be careful, regular expressions are usually expensive in SIEMs. It's can be more practical to be a bit inaccurate and get few false positives, before you kill your SIEM with expensive queries.

Q. It’s a fact that the use of more wilecards lead SIEM to decrease in performance as more event need to be processed. What’s your recommendation in terms of leveraging performance versus rule effectiveness balance (detection rate)? Thomas Patzke: It's hard to find the balance and depends on the rule. If you can reduce the number of wildcards with tolerable increase of false positives, this might be fine. Concrete example from my talk could be matching on "* 1> \\\\127.0.0.1\\*". In the Sigma repository we prefer more accurate rules. Depending on the environment, each one can adapt the rules as required.

Q. Are there are regex in sigma? Thomas Patzke: You can do this with the value modifier "re", e.g.: CommandLine|re: '.*foo.*bar' Docs: https://github.com/Neo23x0/sigma/wiki/Specification#value-modifiers But be careful, regular expressions are expensive and can decrease performance of your SIEM!

Q. Is it possible to create Splunk-CIM base query? Thomas Patzke: Configurations can be used to map field names and add conditions based on the log source. This could be a solution, but as far as I know nobody has contributed this until now.

Q. How do we test the sigma rule after creation if we don’t have Splunk? Assume we just use it locally with winlogbeat? Thomas Patzke: I've created a small side project, the ELK detection lab for this purpose: https://github.com/thomaspatzke/elk-detection-lab - It uses some public datasets, Mordor, Samirs EXTV Attack Samples and Suricata-processed PCAPs from malware-traffic-analysis.net. There's also Splunks Attack Range Patrick presented today, which includes Splunk: https://github.com/splunk/attack_range

Q. Is there any ongoing or planned development to increase the coverage of Attack navigator by adding Attack for ICS TTPs? Adam Pennington: Yes. ATT&CK Navigator leverages the STIX representation of ATT&CK. ATT&CK for ICS isn’t yet available in a STIX form, but once it is (hopefully later this year) we will be extending Navigator to support it.

Q. Are the training and evaluation dataset available so we can replicate the results, port to other ML frameworks and integrates in tools? Connor Magee: They will be when the new update to tram is publicly released!

Q. Tram: What type of file formats does it support? Connor Magee: PDF, Word documents, txt

Q. Will the export support the Navigator (in the future)? Connor Magee: Yup!

Q. Can we have the link of TRAM documentation? Connor Magee: https://github.com/mitre-attack/tram

EU ATT&CK Workshop Q&A: Day 2

Q. Do you plan to learn your Bayesian network from data? Carolina Adaros: If I can get hold of some data samples, yes!

Q. I implemented a Bayesian network several years ago the challenge was the data requirements to ensure that the network is valid. How are you dealing with the data issues to support the probabilities in the network? Carolina Adaros: I am still not there, so far I just did a prototype example which was more focused on the model than the specific data so I used some synthetic inputs. But on a real implementation that is an issue. There are some methods to calibrate probabilities based on educated guesses, but at the end of the day risk management is not an exact science I am afraid... I mean risk = dealing with uncertainty. And then you have 2 types of uncertainty: How likely is that an event happens within a timeframe? and Is the likelihood estimation reasonable? And the second question will never have an answer. Since the occurrence of the event is binary. You could demonstrate with a lot of data, of course but in ICS targeted attacks you will not always have so much data.

Q. Do you plan release IoRs to public? Carolina Adaros: This year I will probably get a paper published where I elaborate on an example. I am also happy to share what I got so far if someone requests the info directly, since it is still work in progress...but it will be great to get some feedback, if someone is interested on talking a look and have a discussion

Q. I've noticed that you had some techniques like location monitoring or SMS sniffing mapped as 'impact' tactic. Considering actual ATT&CK matrix, this would be more likely mapped as 'data collection' tactic. Can you please share your thoughts on this? Jonathan Olsson: Thank you for your feedback, something to take back for consideration. what you saw is work in progress - definition of tactics (maybe additional tactics needed) is something that needs further discussion, as does mapping of techniques :)

Q. Do you have CTI as the basis for these techniques? Sid Rao: In general, YES! That is how we built the framework at first point. This is mainly how one can understand the operations and strategies. However, we don’t have attack-group specific IoCs… Unlike regular malware that is targeted towards end-user devices, we do not have any publicly sharable IoC/MISP-ish things as of now. This is another reason why we need more participants and data sources.

Q. How well do these work in terms of identifying an attacker through a unique combination of techniques, or is it more a case of categorizing and documenting attacks?

Sid Rao: As of now, we use it for categorizing and documenting attacks. In terms of “identifying an attacker through a unique combination of techniques” is in progress. The public datasets on such things are rare. So, we are working on how to use such heuristics in an open and sharable community effort.

Q. Can you provide the link again for BZAR? Moderator: https://github.com/mitre-attack/bzar

Q. Have you considered creating this using Sysmon? If considered what made you decide to go the Zeek route? Mark Fernandez: No, I didn't consider SYSMON. I chose Zeek because it was open source, so I could add features if needed. For example, I could modify the SMB analyzer to detect or expose a field in the network packet if I needed something above and beyond what Zeek already offered.

Q. Why did they decide to ignore IPC$ share requests. What about lateral movement via custom named pipes? Wouldn't it miss it? Mark Fernandez: Good point. Yes, it would miss that, but looking at the ATT&CK framework, I don't recall if it contains a Technique that uses custom named pipes...? The other part of your question, I wanted to focus on remote access to the file system, the C-drive. Named pipes are more commonly used for tunneling RPC over SMB, so I chose to ignore IPC$. Zeek has such a rich RPC protocol analyzer that it can parse RPC over SMB/named pipes, which allowed me to simplify my scripts.

Q. Do you have a video demonstration configuring or viewing how Bzar works with all the functions configured? Mark Fernandez: No, unfortunately, I do not have a video. There is a README file on the GitHub repo, and the scripts are well-commented to describe the objective or what is happening.

Q. Did you plan to implement ATT&CK in McAfee ePo reports or ENS somehow? Marc Rivero Lopez: That’s a good question. It’s better to reach out to the product engineering team for that as I’m only working in Threat Research department!

Q. Do you include a play book (identify, contain, eradicate, recover) in the development of these use cases? Harry McLaren: We indicate a general generic responsive action, etc. Then in Phantom we have playbooks mapped to alert names for the automation part :)

Q. Will participants receive proof of attendance for the two days? (for continuous professional education) Moderator: The EU ATT&CK Community Workshop has not sought approval for continuing education credits. You may seek approval from your certification body by submitting the program agenda and roster of speakers. Thank you for participating in the Workshop.