

MARS Prototype Usability Study Report

In August 2021, NT4S (New Technologies for Security) - AZA2 conducted two rounds of remote usability study sessions, with 3 sessions in each round. Each session involved one member of the WIM team (either stakeholder or threat manager). The sessions consisted of the moderator (Kendra) first asking general contextual questions to the participants, then asking participants to perform various actions within the clickable prototype. Both the moderator and observer (Laura) asked additional follow-up questions throughout each session. We looked to identify pain points within the MARS prototype where improvements can be made, and prompt deeper discussion on certain functionality within MARS. Since the sessions were done relatively early in the development process, there was a mix of feedback between big-picture functionality and visual UI details.

Methodology

- **Method:** Usability testing walkthrough and observation
- **Remote or in-person:** Remote
- **Number of participants:** 6
- **Session Dates:** Aug 2 - 5, 17 - 24 2021
- **Participant profiles:** First round of sessions involved 3 WIM stakeholders who have previously been involved in requirements gathering and approvals (2 WIM managers, 1 threat manager). Second round involved 3 threat managers who had not seen the prototype beforehand.

User Insights

- **Each threat manager has a unique routine for addressing cases, which we need to accommodate while reflecting their current processes.** Day-to-day threat management work is currently divided between tactical (active investigation, communication with LPs, GSOC, etc., handling cases) and programmatic (logging work, developing trainings, creating reports). Since many of the threat managers are seasoned in managing threats, either within WIM or other areas, the workflow of triaging and addressing cases should reflect their current workflow as much as possible. Instead of abruptly changing their entire workflow with MARS, we want to improve and make their existing process more efficient. We also need enough parity with D3 so the WIM team is comfortable deprecating it and shifting case-related work into MARS.
- **Though MARS is largely built for managing long-term cases, a vast majority of threat management work is spent in direct one-off communications with Loss Prevention parties.** One threat manager estimated that as much as “95-97%” of the time, threat managers are answering quick questions from LP/GSOC or acknowledging cases that have come in with no WIM action required. As noted in metrics viewed in sessions with



stakeholders, around 80% of current WIM Incident cases have already been appropriately handled by local LP and do not require any threat management action. In addition, nearly all SEV1 and most SEV2 cases coming from GSOC would already have a direct SEV call with a threat manager or other direct communication and management before the report is submitted through EMT. This amount of direct communication that threat managers receive while on-call means that their attention is often split and distracted between different applications, so we want to ease these communications within MARS. With the foreseeable high usage of the Consultations feature, there should be additional intentional thought and review of its workflow.

- **Threat managers find MARS as a helpful “one-stop-shop” for case information, but may prefer to go out to other services directly for further investigation.** In their current workflow, threat managers often switch between the multiple applications of CMS, D3, Loss Prevention directory, Admin Directory, Chime, email, and SIM Ticketing. One of the values of the WIM team and major goals of MARS is to integrate the information from these different services within MARS. A few of the participants mentioned use cases where they would want to do further investigation in these external services directly, so we should not only bring in information from these services, but provide easy links for external investigation.
- **The WIM team values metrics to both track case information and capture the work spent by threat managers.** In their current workflows, the WIM team must put together case data from D3, CMS, and EMT to produce meaningful metrics and to identify trends. We are improving their experience in MARS by providing robust data that they can quickly download reports from, and metrics visualization that would help them to better identify trends earlier. They use these metrics to inform decisions on the types and locations to provide additional training, and to anticipate threats before they escalate into dangerous incidents. The other element that the WIM team looks to track is the distribution of where threat managers are spending their time while working. Currently they manually log their work through Quip docs, as well as log any engagement with other parties in D3. We have an opportunity in MARS to embed this data in explicit assignees and track the amount of logged consultations per person, with which WIM leadership can run reports.

Positive Feedback (+)

- **The MARS UI unanimously matches the mental model of how threat managers prioritize cases.** Throughout the sessions, participants had a similar order of how they would address cases: new → updated → general open cases/my cases, and highest severity/level of concern → lowest severity/level of concern. Both the [dashboard](#) components and the order of Case lists in the sidebar match this logical order, and will ease threat managers’ workflows when first opening MARS when their shift starts. Besides a few additions, the MARS UI also displays essential information participants were looking for to learn the basic information about a case in the lists and case details box: event type, category, subcategories, time of incident, location, recency, flagged



words (the “what, when, where”). Participants noted that the steps of case triage also closely reflect what they’re used to in their current process.

- **There are helpful micro-interactions throughout MARS that will contribute to a more efficient workflow for threat managers.** In [form fields](#) specifically, the ability for employee information to be auto-populated from searching by alias, auto-populating facility information based on facility code, and the ability to start typing to filter the results within a Meridian Select component, all were found to be delightfully easy for participants to use. We should continually look to micro-functionality that we can make more efficient for a better overall experience for users.
- **MARS offers robust [metrics and reporting](#) capabilities that would benefit WIM research and identification efforts.** With the amount of data fields that can be used to filter case data, the WIM team is excited to have one central place where they can run routine and on-demand reports, to the point where one participant “wished I had this” at the time they had previously struggled in creating reports for a case research project.
- **Logging [consultations](#) is an easy and quick process**, contrary to the current cumbersome process of logging an entire case in D3.
- **The functionality of [bookmarking](#) cases was easily understood and navigated.**
- **The second round of participants understood and easily located the [Related](#) tab to look for linked consultations and cases.**

Opportunities for Improvement (-)

- **Reorganize the workflow of acknowledging updates to improve accountability and maintenance of updated cases. [RESOLVED]** One of the WIM managers thoroughly discussed the importance of compliance in each threat manager having explicit ownership of cases and documenting all of their actions. The initial structure of acknowledging updates in MARS was each user dismissing cases on their own Updated Cases list. Although this was intended to ensure that each threat manager has visibility to each update that comes in to open cases, there was concern that this didn’t provide enough explicit ownership and there was a possibility of an update to be lost if every TM dismissed it. This acknowledgment mechanism has been moved into the [case details](#) itself, where a user can explicitly acknowledge an update and the [Updated Cases list](#) will be shared among all threat managers.
- **Restructure the content of the [Persons Involved](#) tab to improve organization and declutter the information presented for each person. [RESOLVED]** When asked to add a contact to a case, all three of the first round of sessions did not notice the separation between the persons involved and contacts sections. This warranted a restructure of these sections to create a clear separation between the people that were involved in the case (persons of interest, victims, witnesses) and contacts associated with the case, while having a single “Add person involved” button to cover both of these roles. There was also common confusion around indicating which persons involved/contacts were manually added vs automatically imported from EMT, so we included “Added by...” and a well-understood edit button to explicitly indicate these. Along with these changes, we



improved the unnecessary amount of information presented about each person by nestling basic information within a clickable popover, with links to external services if further investigation is needed. After these changes were implemented, the second round of participants easily navigated to add a contact, and appreciated the clean presentation of persons involved. One of them also noted that they find tenure and employment status as important to assessing how they should address certain persons involved, so we replaced phone number and email with this information as it is more helpful to threat managers.

- **Change the design of how suggestions are presented. [RESOLVED]** In the first round of sessions, there was prominent confusion around the button elements of accepting & rejecting a suggestion for assigning a case, linking a SIM ticket, and linking a consultation. Instead of appearing as clickable buttons, the component appeared to participants as a check-marked element that was previously added to the case. This prompted a change to [nestle suggestions into the search input fields](#) for these three elements, so it's a cleaner UI and consistent.
- **Provide easily-accessible information to contact the responsible LP for each case.** All three threat managers in the second round of sessions made a clear point of how the current MARS prototype did not display the responsible Loss Prevention contact, which they nearly always contact to get more information or discuss the nature of each case. This will be an added sidebar component in the next round of prototype edits.
- **Possibly restructure or shift where the [Summary](#) tab information is presented.** There was some mild feedback of participants being slow to navigate to the Summary tab to learn the basic information about a case. One of the threat managers specifically referenced a system he had previously used in law enforcement where everything regarding a case was presented in a single column, continuous-scroll page to create a clear story upon read-through. From this suggestion, there could be a change to making the Updates thread one continuous scroll (with loading animations) rather than paginating. This will help to create a clearer mental timeline of updates in a case, and it rarely will become overwhelming as most of the cases threat managers handle will have a small number of updates. There is a possibility of combining the Summary and Updates content, but will require additional feedback to make such a large structural change.
- **Possibility of better explaining the [Recommendations](#) tab.** There was some confusion of threat manager participants in whether the Recommendations were what LPs had already provided to the case, or for TMs to document their recommendations to a case. This could be a simple solution of labelling, or could warrant some ability to pull out LP recommendations through the form to EMT.
- **Add "Proximity" as a data field in each [case listing](#).** This was a common request from threat managers to help them better understand the basic context of a case.



Topics for Follow-Up

- **The WIM team will need to clearly standardize the triaging steps of all cases, balancing accountability and efficiency for threat managers.** The two actions the current MARS UI expects threat managers to do for every new case that comes in is to set a level of concern and assign it to a specific threat manager, before doing any further updates or closing the case. Although this provides clear accountability and produces cleaner metrics, since a majority of cases require no action by threat managers, the TMs in the second round of sessions were concerned with this required manual effort being overwhelming for the large case load they work with. After discussion with the WIM team, they will discuss this further internally and decide what manual actions they expect threat managers to do for every case, and we will adjust the UI accordingly.
- **The WIM team will need to clearly communicate the differences between a [MARS investigation case](#) and a [consultation](#), and train for what circumstances each should be used.** After discussion with participants, there is a gray area in the circumstance of an LP reaching out to a threat manager, and the situation is pre-WIM incident but could quickly escalate. In this instance, a threat manager could either record it as a one-off consultation or open a MARS case for ongoing investigation. In either situation, we account for changes as the situation evolves through the ability to link cases to each other and link consultations to cases. Because EMT should be the source of truth for every Ops incident, the MARS investigation case should only be used to track on going threats that are not yet a WIM incident. Therefore, we will be adjusting the fields in the create case form to be less post-incident as in EMT, but rather pre-incident, with care as to how these fields affect metrics.
- **We will need to be in contact between the EMT and WIM teams as EMT 2.0 rolls out, specifically around the categorization and labelling that EMT 2.0 will be using.** Historically, security risk analysts (SRAs) within GSOC often mis-categorize incidents into Security, Medical, etc when they should be WIM Incidents. In discussions with stakeholders and participants, rather than bringing in all security and medical incidents which would dilute the cases that need WIM attention, the WIM team will be discussing which specific criteria of cases — category or otherwise — they want to be brought into MARS. Threat managers also made the point that the WIM team shouldn't act as "babysitters" for SRAs, but should actively be clear with GSOC to encourage more accurate categorization during initial reporting. There is opportunity for discussion on how EMT 2.0 will accommodate changes to categorization if the WIM team requests.
- **Encourage EMT 2.0 to provide an easy process for LPs to record incident directly into the tool.** This would solve the problems of LPs making numerous direct contacts with threat managers rather than recording incidents through the standard process, and the time delay it takes GSOC to log incidents in EMT
- **We need to thoroughly test MARS in different browsers.** While running the sessions, participants use a mixture of Google Chrome and Mozilla Firefox, so MARS should accommodate and perform well on either of these browsers, as well as others.



Appendix

Reports & Materials

- Sign-up Document: [MARS User Research Sessions](#)
- Task & Question List: [MARS User Research Tasks](#)
- Individual Finding Reports
 - First round (stakeholders)
 - Naomi: [Usability Testing Findings - Naomi](#)
 - Brent: [Usability Testing Findings - Brent](#)
 - Dawn: [Usability Testing Findings - Dawn](#)
 - Second round (threat managers)
 - Jeff: [Usability Testing Findings - Jeff](#)
 - George: [Usability Testing Findings - George](#)
 - John: [Usability Testing Findings - John](#)
- Prototype: <https://xd.adobe.com/view/b08771b1-7dbb-46c0-bf77-4308ff38df57-e5d4/>
- SIM: <https://sim.amazon.com/folders/7fbf1168-b176-4eb2-8e29-d0520c78d57f>

Stakeholders

- **Researcher/Designer:** Kendra Raczek (kraczek)
- **Product Manager:** Laura [REDACTED]
- **WIM stakeholders:** Dawn [REDACTED], Brent [REDACTED], Christian [REDACTED]
[REDACTED], Naomi [REDACTED]

Script

Introduction:

- How it will work
- Testing the prototype, not you
- Scope for visual elements and organization rather than functionality
- Static data
- Recording

Context questions:

- How long have you been a threat manager?
- What region/location do you specialize in?
- What current applications do you use to do your day-to-day work?
- Your method for working through cases (seems like TMs different)?

Scenario:

1. Just after clocking into work, you pull up the dashboard to view the high-priority notifications.



- a. What do you make of the cases listed? What information are they presenting?
 - b. What do you tackle first? How do you decide, what do you look for that you most quickly want to address?
 - c. After addressing all high-priority cases, where would you go next in your daily work? What's the next most important task for you?
2. While triaging new cases, you open up a new case for the first time. (MARS)
 - a. What are the first places your eyes go when looking at the case details page?
 - b. What places would you first look to learn more about the case?
 - c. How would you learn more about the person of interest? What info are you looking for?
 - d. Based on what you see on the page, what steps would you take to do the initial triage?
 - e. At what point would you feel comfortable assigning it a level of concern?
 - f. You notice that the location of the incident is not in your AOR. You assign it to the appropriate threat manager.
 3. Checking through the list of updated cases, you notice and want to look at an update that came through SIM.
 - a. It has some alarming flagged words, look for where they were used.
 - b. Acknowledge the updates.
 - c. You see an alarming Facebook post someone from GIP attached to the ticket, and decide to increase the level of concern.
 - d. In addition, you believe it's necessary to recommend adding more physical security to the facility where the POI is.
 4. You've recently received a call with an LP on an associate's concerning behavior. They have been grumbling about their manager to other coworkers with possible threats, and might act out in the near future. (New MARS case vs Consultation)
 - a. Case or consultation?
 - b. You'd like to record the details of this conversation in MARS for record-keeping.
 - c. Later, a new case comes in with the same associate as the POI. Link this case with the consultation you added.
 - d. You'd also like to record this LP as a contact for anyone working on the case as it goes on.
 - e. Someone else is already assigned to that case, but you want to save it somewhere to in case you need to do any work on it in the future.
 5. You end up with some available time toward the end of your shift and want to look into some possible trends that you've been noticing over the past month or so.
 - a. You do a simple search to look up kidnappings that have happened in the AZA2 facility.
 - b. The simple search doesn't end up providing very accurate search results, so you decide to do an advanced search - What fields do you choose? How are the advanced filters organized? Can you find the fields you're looking for?



- 276 c. The advanced search result cases appear and it confirms your suspicion that
- 277 AZA2 has had an influx of kidnapping cases in the past few months
- 278 d. You want to investigate this further to examine this specific trend over a larger
- 279 time period - where would you go to look into this?
- 280 e. On the metrics page, how would you view a line graph for kidnappings in AZA2
- 281 or a broader location like Arizona or AMER?
- 282 6. You are a MARS admin and recently hired someone to be in another admin role.
- 283 a. Set this person's area of responsibility to AMER central since that's the location
- 284 they have experience working with.

