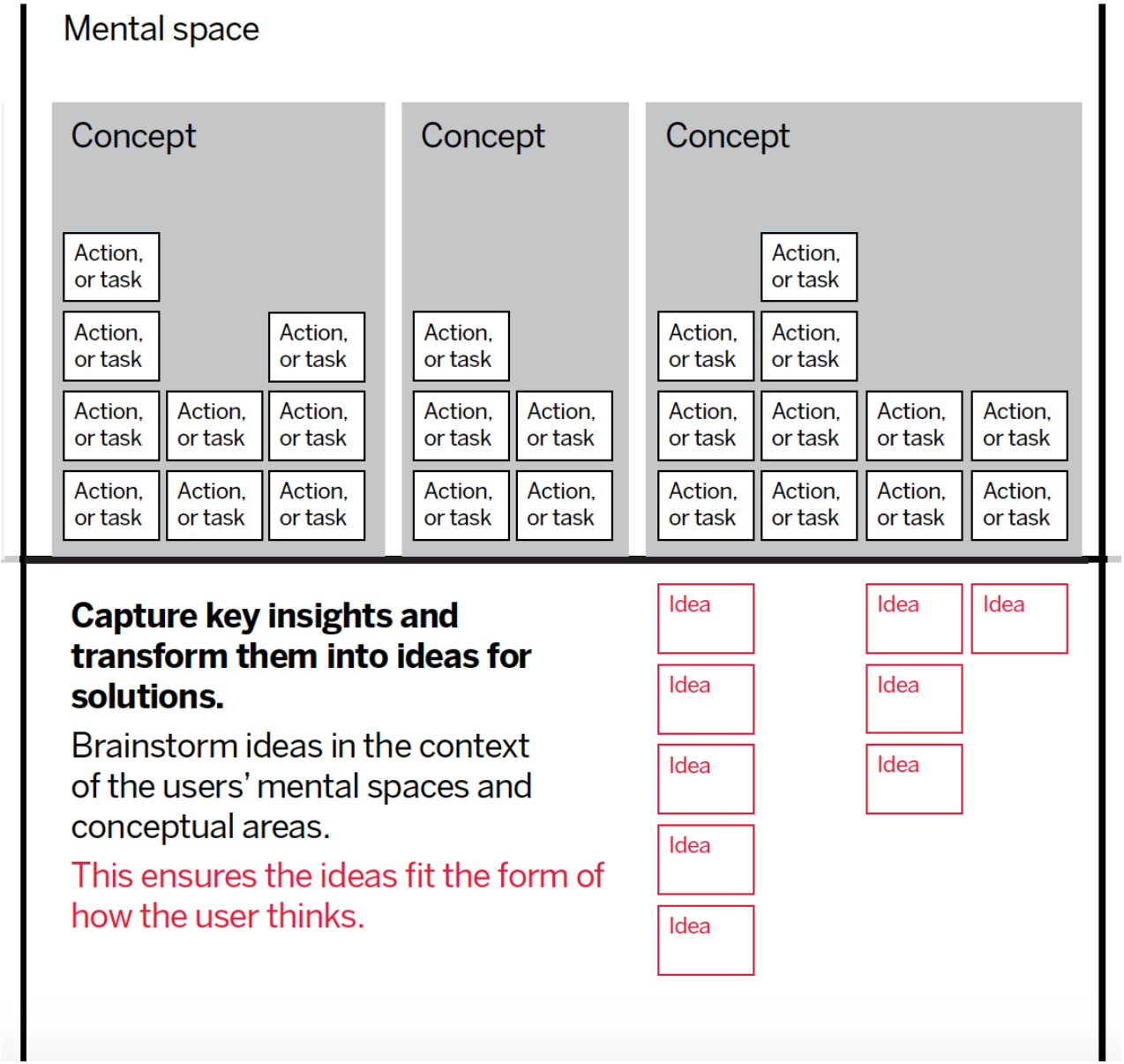
ENDGAME.

COP Users Mental Spaces

December 2015

How to use this doc



Mental Space
Patterns among target users around how they organize their thoughts and actions

Concept Area
Related tasks or actions within a mental space are grouped into concept areas

Tasks / Actions
Individual things a user does related to a specific activity

MENTAL MODEL LEGEND

- Domain area
- Domain concept
- Key point
- Focus for first release

Mental Spaces

1 Managing

Managing is the process by which a user organizes their own workflow and includes how they approach their daily tasks. Due to its tactical nature, this area only includes how they organize their files, corresponding folders and their time.

2 Triaging

Triaging is the process of deciding what thing or things are most important and how to manage competing priorities and needs. This also includes handling context switching and is mostly confined to a single user and their own methodology (i.e., does not usually involve collaboration)

3 Reporting

This entails the creation of any and all assets after an incident and the act of sharing those findings with others both inside and outside of the organization.

4 Collaborating

Collaborating is about working closely with others, particularly as it relates to a mission or an investigation. Typically this is the sharing of information between analysts and operators although it can include other individuals outside of these roles.

5 Responding

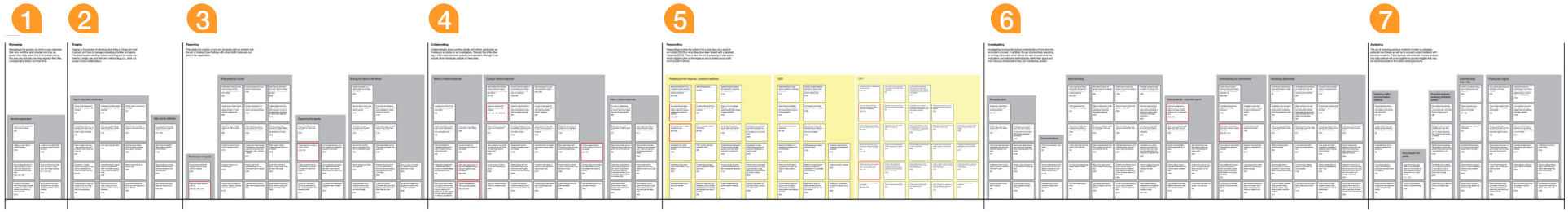
Responding involves the actions that a user does as a result of an incident [DCO] or when they have been tasked with a targeted mission(s) [OCO]. There is also the act of preparing to take action which happens prior to the response and is shared across both OCO and DCO efforts.

6 Investigating

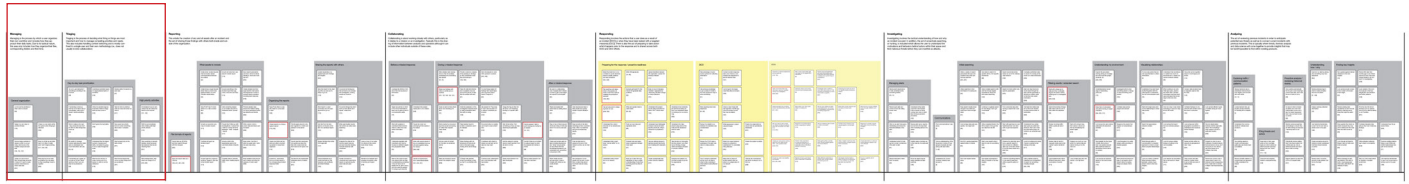
Investigating involves the tactical understanding of how and why an incident occured. In addition, the act of proactively searching, or hunting, is included which allows the user to understand the motivations and behaviors behind actors within their space and find malicious threats before they can manifest as attacks.

7 Analyzing

The act of reviewing previous incidents in order to anticipate potential new threats as well as to connect current incidents with previous incidents. This is typically where trends, forensic analysis and data science will come together to provide insights that may be hard/impossible to find within existing products.



Managing & Triaging



Managing

Managing is the process by which a user organizes their own workflow and includes how they approach their daily tasks. Due to its tactical nature, this area only includes how they organize their files, corresponding folders and their time.

General organization

- Let me set the priorities of what I want to secure [59]
- Assign my own value to potential threats [175]
- Create my own alerts within the system when things get detected [168]
- Remove large numbers of dupes in order to cut out noise, then focus on the smallest unique set available. [194, 195, 197]
- Keep to-do list up and refer back to it often to make sure I don't forget anything [317, 318, 319]
- Create my own tools to filter through large amounts of data b/c I need to make special connections between data sets [201]
- Bring back as much data as possible into one place so that everything I need is together [202]

Triaging

Triaging is the process of deciding what thing or things are most important and how to manage competing priorities and needs. This also includes handling context switching and is mostly confined to a single user and their own methodology (i.e., does not usually involve collaboration)

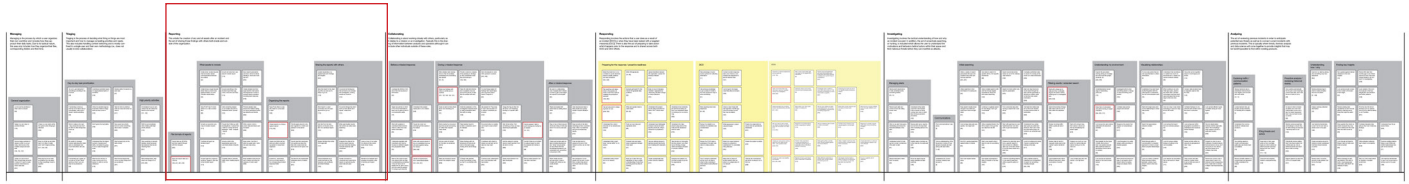
Day-to-day task prioritization

- Try not to get distracted if something is working in the moment. [49]
- Understand priorities based on organizational matrix of severities [104]
- Review alerts I've saved at a later date [97]
- If something comes up that has to be taken care of immediately, make sure it doesn't derail everything. [50]
- Utilize the severity/orgnization-al alert matrix to triage alerts as they come in [105]
- Take the time to prioritize what we need and when we need it [257]
- Work to balance the load - stay productive but don't be blind to other things that come up. [52]
- Don't ignore the bad alerts [162]
- Save super low priority items for when everything else is slow / complete [283]
- Be careful to manage context switching and make sure to understand how much that switch will cost. [54, 55]
- Understand that the higher number of sensors and traffic, the harder its going to be to wade through the noise [169]
- Stay focused only on the task at hand [291]
- If something isn't useful, let me bail out of that "thing" quickly so that I can continue to be productive [58]
- Minimize the amount of noise coming out of my system in order to not be distracted [170]
- Work around issues that come up when things don't go as planned [307]

High priority activities

- Immediately focus on process-es that are clearly the result of a live human [101, 102]
- Shift focus immediately when dealing with high-priority attacks [176]
- Drop everything to remedy situation when someone has detected that we are watching them [227]
- When things break, drop what I am doing to fix it [259, 282]

Reporting



Reporting

This entails the creation of any and all assets after an incident and the act of sharing those findings with others both inside and outside of the organization.

What assets to include

- Create short, tactical reports that summarize simple communications between two entities [32]
- Include all notes from analysts in incident report [114]
- Save search parameters and how I arrived at those results (ie, what was I looking for?) [205]
- Create broad, longer reports when there is a new investigation/mission or more complex relationships. [33]
- Include everything in the incident report like logs, notes, executive summary [115]
- Create detailed and thorough reports of all events that happened in order to recreate attack scenarios including team response [219]
- Save PCAP that I'm interested in to a file to review later [98]
- Grab everything related to an incident and all it to theshared folder / journal [153]
- Provide detailed data around the mission during my report generation including statistics and trends [260]
- Include an executive summary in incident reports [111]
- Ensure that I follow up with investigations / actions that I start by coming full circle (signature - data - analysis - report) [177]
- Write custom code to crunch data and return useful results [268]
- Combine all logs in an incident report [112]
- Include a link to the signature(s) used in the comments fields of reports [179]
- Keep notes / text file of what my goals were / what the team was doing [302]
- Include logs from everyone working / logged in that day in the incident report [113]
- Correlate data to network traffic when creating reports [191]
- Keep detailed notes around each mission including the versions of tools I used [308]

Organizing the reports

- Keep PCAp files in a specific folder to come back to later [100]
- Create reports in a chronological manner [110, 216]
- Pull all assets around a mission together in a folder and upload it to the server [303]
- Create one folder per incident and utilize a numbering system to keep them organized [116]
- Export data from previously run queries and save the files with a name that ties them back to the query I ran [279]
- Include ALL information from an incident report in the corresponding incident response folder [117]
- Put files into the appropriate databases when a mission is over. [327]

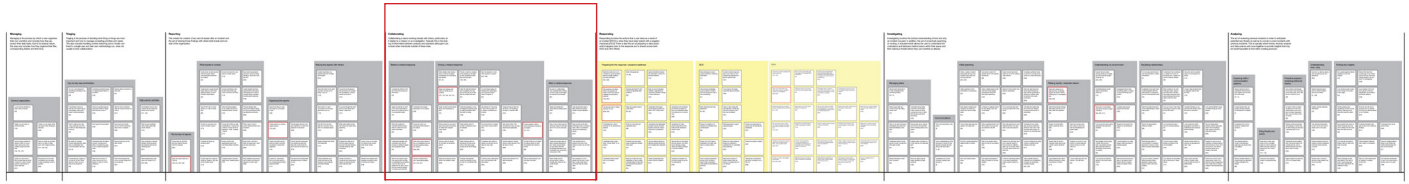
Sharing the reports with others

- Update leadership on a regular basis with findings and insights [042]
- Send the report to the clearing office as soon as it's ready to go out. [118]
- Document all findings so that someone can recreate the investigation / finding exactly as I found it [154]
- Send report to cyber command once it's been approved to go out [119]
- Document things that didn't work so that others don't repeat / waste time [155]
- Get intel from the intelligence community in the form of a serialized report. [135]
- Write searcheable reports that others can utilize when searching [180]
- Review findings from other DOD agencies [147]
- Snapshot the data at the time the search was run and use that when sharing example searches with coworkers [209]
- Leave a copy of my notes for others so they understand what I found. [265]
- Create shareable documents (journals) so that everyone can contribute and share findings [152]
- Explain decisions to coworkers and supervisors based on reproducing the exact data set used [210]
- Monitor and evaluate team progress via weekly notes of activity and impact [346]

File formats of reports

- Export data as JSON file and then search through JSON in notepad [232]
- Save and export data as a CSV file [183, 231, 267, 278]

Collaborating



Collaborating

Collaborating is about working closely with others, particularly as it relates to a mission or an investigation. Typically this is the sharing of information between analysts and operators although it can include other individuals outside of these roles.

Before a mission/response

- Leverage the efforts of others to find new sources of information [45]
- Target sys admins or other in-the-know individuals to learn how to gain access to communication paths [14]
- Understand the analyst needs prior to the mission [350]
- Work with analysts to understand their needs in order to collect the most useful information [28]
- Ensure the tools I am developing fir the needs of the analyst [254]
- Collaborate regularly with coworkers who may be focused on different targets and geographic areas. [35]
- Work with analyst ahead of time to understand how we will work together during the mission [286, 300]
- Seek to find ways to learn how unique roles can help in understanding something I may not have a lot of insight into (ie, talk to someone who uses the system I'm trying to get into) [44]
- Get list of requirements from customers/analysts [331, 334, 337]

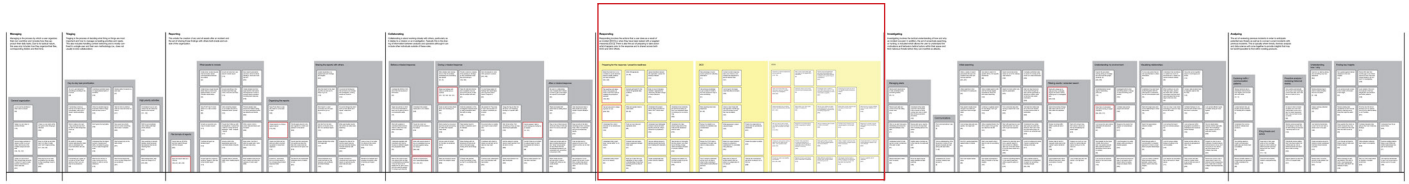
During a mission/response

- Write detailed alert descriptions so that the analysts understand why something was alerted [76, 78]
- Provide context to analysts when passing on findings so they understand what they are looking at. [190, 196]
- Send developers to work with operators in person [343, 349]
- Share key findings with follow-on shifts and coworkers [131, 132, 149, 150, 151]
- Pass off collected information to analysts once we have all the pieces of data that the analyst will need. [27]
- Try new things based off findings from teammates who may have ideas I havent' thoguht of. [43]
- Open an alert so that others know I am reviewing the alert. [73]
- Enlist the assistance of the investigaiton response team to really understand what the traffic is doing. [109]
- Ask analyst for Pcap data if I don't have access to it in order to understand an incident. [123]
- Chage the flag so that others know I am reviewing/tending to a specific alert [125]
- Work smarter by documenting what people are looking for rather than repeat it many times. [130]
- Pass binaries found in emails to analysts to see if its malware [136]
- Document when no results came back to save others' time [156]
- Alert others when I find something so they can stop searching (if applicable) [158]
- Quickly assess if alert is worth looking into further by an analyst [74, 127]
- Act as a point of contact for the team via email and phone [258]
- Share findings with collabortaors so that we are both on the same page looking at the same things. [266]
- Coordinate with others to ensure we pull back all the data we may need [272]
- Ask the analyst to decide what is most important if we are short on time [298]
- Decide if there is an incident to analyze based on what the analysts felt merited a review. [66]
- Make the decisions quickly when/if an analyst is away [299]
- CONSult with analysts when/if something comes up that I'm not familiar with [301]
- Continue open collaboration and communication with teammates [305]
- Divide work between multiple developers [338]
- Split up tasks between various team members [340]

After a mission/response

- Be open to collaborating even if targets aren't shared in order to gain more insight into specific technologies [36]
- Share successes with teammates by talking about them [41]
- Uses reproduced data to train people and quickly explain a search situation [211]
- Stay on top of what org and others are doing in their jobs (even if it's not my own job) [96]
- Keep records of dat after searching so that coworkers trust / utilize my searches and the accompanying results. [213]
- Create and update alert details including descriptions and "whys" around alerts so that others with less knowledge/experience can understand why something is important [129]
- Push all data back to analyst at the end of the mission so they can do their jobs [28]
- Share details around process when I made a mistake with others so we could all learn [304]
- Ask operators to come speak with his team to give them a better idea about how their tools are being used [345]

Responding



Responding

Responding involves the actions that a user does as a result of an incident [DCO] or when they have been tasked with a targeted mission(s) [OCO]. There is also the act of preparing to take action which happens prior to the response and is shared across both OCO and DCO efforts.

Preparing for the response / proactive readiness

- Select the best time to run a mission to avoid detection based on traffic patterns and user behaviors [324, 326]
- Write IDS signatures [75, 80]
- Upload identified malware into orgnization system for tracking malware [137]
- Run searches and signatures in the sandbox in order to test them without crashing the production systems [146, 285]
- Exclude particular IPs that I know will generate false positives [82]
- Keep on top of changing malware / signatures because they will often change to evade detection [161]
- Test all tools prior to releasing them for use. [248, 339]
- Write and update rules to catch alerts [84, 85]
- Understand the system we are using and what the alerts / info / colors mean [164]
- Understand how networks are named and setup so that I can understand what I'm looking at on a comms map [322]
- Understand the current structure of my network and sensors [165]
- Push out new rules and signatures often [86]
- Understand and distinguish between normal and alert-specific activity (ie, what's normal for my systems?) [165]
- Understand the risks around using each of the tools and the decisions I need to make [310]
- Understand what constitutes "normal traffic" in my system [167]
- Forward rules and signatures to signature management team [87]
- Use pre-defined groups to estimate severity (and priority) of dealing with attackers [174]
- Take the time to thoroughly test the product I am creating by thinking of edge cases and staying focused on product delivery [252]
- Understand what's important in my network [60]
- Keep up to date with new signatures to have a better understanding of what they are doing and how they're working [95]
- Create operationally-supported tools for missions [247]
- Authorize the release of a tool that is ready to go into the organization [249]

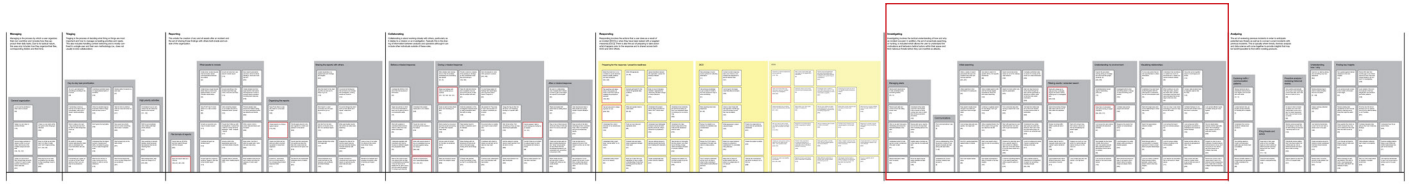
DCO

- Take advantage of open-source options for collecting information [11]
- Contact incident response team once I know a compromise has happened to get the relevant logs. [107]
- Use previous knowledge to get a sense for what is the most productive way to solve something [51]
- Comb logs to find suspicious files after an incident. [108]
- Block anything that looks suspicious [67, 68]
- Check to see if base still had logs from months ago once an incident occurs that may be related [122]
- Review the details to understand if a harddrive was compromised [69]
- Write signatures to detect network threats [133]
- Ensure the organization is secure from an operational standpoint [251]
- Review the PCAP data to understand if the alert was valid or a false positive. [72]
- Watch for unsual behavior around my network to understand if I'm potentially being attacked [225]
- Ensure the system is stable [255]
- Once a breach is detected, pull as much old data in order to fully understand what systems were affected and how. [94]
- Make sure to patch all similar systems after an attack on a single place in my network [243]
- Capture the commands a sys admin is using to try to find me [296]

OCO

- Continue to improve signatures as time goes by [138, 139]
- Ask if what I have really gets me closer to the targets that I care about [5]
- Review excel spreadsheets and word docs particuarly those that have been recently modified when performing an investigation [221]
- Open and review files that have been recently modified during my investigation [235, 222]
- Intercept online communications and pull necessary data [8]
- Investigate when I believe I have been discovered or I feel someone is tracking my movement within a system. [261]
- Protecting the tools we use is the highest priority during any mission [292]
- Assist operators by providing remote troubleshooting of tools [341, 342]
- Task entity once I find what (data) I'm looking for [25]
- Get as much detail and data as possible when I am doing an investigation including why something happened [262]
- Keep track of tool versions and the staus of those tools [309]
- Save time by running multiple scans through different computers [316]
- Set up a way to return when my mission entails just getting back into the system at a later time [145, 290]
- Respond to important items when a response is merited [134]
- Use my toolset to gain access to other computers [284]
- Pull files when missions only require assets to come back [312]
- Respond in a timely manner particularly when something changes [321]
- Initially just worry about pulling back as much data as possible - ask questions later [240, 273]
- Perform data operations on data coming back to understand what's going on especially when anomalous activity is occuring [185]
- Make getting files a priority when the job entailed gathering actual artifacts [288]
- Utilize multiple machines when working within a single mission where necessary [314]
- Create alternative or unknown routes between assets to be more efficient [323]
- Ensure my work is as stealthy as possible [253, 256, 293]
- Maintain known good result sets in response to searches [212]
- Make efficient exploration a priority when the job entails just looking around [289]
- Use single machine-task instead of tryig to do everything on one machine, ie, get only files with one machine [315]
- Focus on specific set of hardware [351]

Investigating



Investigating

Investigating involves the tactical understanding of how and why an incident occured. In addition, the act of proactively searching, or hunting, is included which allows the user to understand the motivations and behaviors behind actors within their space and find malicious threats before they can manifest as attacks.

Managing alerts

- Review alert descriptions to fully understand why something alerted [79, 77]
- Review each alert as it comes in from the rolling screen view. [70]
- Understand what alerts come from live humans in the moment vs those coming from bots or other (less-timely) automated processes [103]
- Click on an alert that seems interesting and review the transcript (details) of the alert [71]
- Review alert name, description and why it's important when reviewing alerts in the queue [124]
- Understand what I'm looking for in order to determine if the alert is valid [81]
- Quickly make a decision as to the veracity of a particualr alert [126]
- Review transcript of alert that I've saved. [99]
- Know the alerts that are easily classified as false positives. [128]

Communications

- Find communications I care about. [3]
- Get an understanding of the big picture in terms of how groups of people are interacting with each other. [1, 62]
- Understand the communications I already have access to [6]

Initial searching

- Utilize a variety of search parameters like type and modified date when performing searches [220, 223]
- Use dates to search for specific alerts or for specific timeframes [89]
- Search abnormal activity based on out of the ordinary user behavior [199]
- Contiually pull/refresh data to ensure I'm looking at the most up-to-date information [226]
- Utilize searches to find information I'm looking for. [24]
- Utilize multiple search methods that include regular expressions, filters and text-based searching. [143]
- Search for items within very specific parameters [203]
- Start very high-level and move down through the data until the granularity is almost too small in order to find the most useful information [229]
- Keep search results broad enough to be useful (i.e., make sure I have enough data) [31]
- Continue to vigilantly search for new things / don't get comfortable [163]
- Find connected data after running a search that I care about [206]
- Use high-level initial data set to find more interesting data points worthy of exploration [269]
- Look at large data sets very quickly / at a high level [56]
- Utilize metadata fields in the DB to search, then pull the raw data from the DB [181]
- Start with searches at a very high/broad level and then work to get more specific [207]
- Understand how certain data types are pulled and stored so that I don't miss key information that is formatted in an unfamiliar way [270]
- Run SQL queries (searches) against areas of interest [65]
- Start a new search when I want to look into something new [182]
- Preserve the data that came from a specific search in that moment b/c different data may come back when/if I run the same search at a later time [208]
- Look for multiple pivot areas / facets to explore when looking at the data [277]
- Don't use regular expressions [88]
- Use regular expressions if data is complex to find key insights [187]
- Looks for everything relating to one search parameter within a specific period of time [214]
- Utilize multiple systems (classified and unclassified) to search for something including Google [332, 333]

Filtering results / extended search

- Start with a large set of data and then continually dig into the data to shrink working set to a manageble size [228, 204]
- Spend time sorting through data when there is a lot of data within the database. [30]
- Review incoming traffic within a particular set of data. [64]
- Start with a broad view, then narrow it down but then try broadening the search again [244]
- Review data by hand or manually review each entry if server cannot transform data [186]
- Analayze as much as I can within my current data set before moving on to the next one [281]
- Links results/events within different data sets to draw conclusions of events [215]
- Look at large data sets very quickly / at a high level [56]

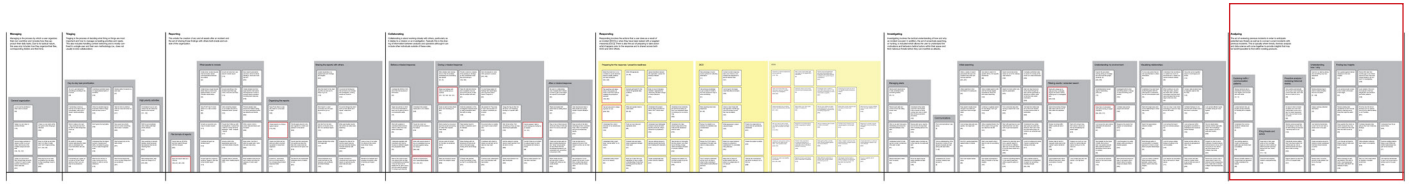
Understanding my environment

- Explore the processes running during an investigation with tools like google, virustotal, etc [238, 239]
- Understand/grow knowledge of networking protocols. [7,9]
- Investigate further when something starts to change or does something unexpected [160]
- Keep track of processes and users running on target machines [294, 295, 311]
- Correlate data across plugins and sensors [192]
- Let me see into user actions particularly the abnormal activities [61]
- Sequence the events that happen on networks/systems [217]
- Have insight into the types of traffic and ports so that I can quickly exclude false positives based on information I know about my system [83]
- Look throughout my entire system when somethig of interest appears [245]
- Look across the network/assets to find bad domain names [142]
- Work around the shortcomings of our system which doesn't allow for testing things out ahead of time [306]

Visualizing relationships

- Find access points that provide opportunities to collect information. [4]
- Understand that sometimes no matter how much we look there isn't a viable connection between entities [38]
- Group like-actors together based on techniques and tactics [173]
- Understand how each layer works/integrates with the other layers to understand the full communication path [16]
- When working in an unfamiliar geo space, seek to see where else a familiar technology may have been used and apply that knowledge to this new area [46]
- Connect data received back to signature used to find the data [178]
- Start with single data point to find relationships to other data points. [19]
- Give me a way to see where technology is used at a high level in the world [57]
- Correlate findings on one network with another even if they aren't connected [184]
- Look across different types of entities during an investigation [242]
- Search for associations between entities [20]
- Look across the board / from an overview perspective [63]
- Look across and within geographic boundaries to understand local nuances behind findings [193]
- Dig into relationships between entities especially when I find something I didn't expect to find in a particular location [263]
- Work through paths of communication in a layered-approach in order to understand complex relationships [34]
- Look for unique outliers instead of looking at the commonalities [140]
- Review activity within my network via geographical view / map [224]
- Expand my view to see a multitude of hosts/locations that someone is on (ie, don't focus only on one device, esp if the person is on multiple machines) [297]
- Look at a variety of relationships between entities (globally, outside of geo area) in order to find new insights. [37]
- Look deeper into something that is rare and/or in fewer places [141]
- Chain events and data together in larger views to get a birds-eye view of relationships [230]
- Review the comms map in cases where I need to understand what is happening from a high level or across multiple machines/networks [320]

Analyzing



Analyzing

The act of reviewing previous incidents in order to anticipate potential new threats as well as to connect current incidents with previous incidents. This is typically where trends, forensic analysis and data science will come together to provide insights that may be hard/impossible to find within existing products.

Exploring traffic / communication patterns

- Review historical data to understand trends around how targets communicate with each other. [12, 13]
- Locate relevant intel, particularly across networks, for handing off to analysts [2]
- Understand the communications I already have access to. [6]
- Use existing assets to model communication paths (aka use what's readily available) [15]
- Review all traffic related to a compromise that happened to fully understand the breach [90]

IDing threats and actors

- Keep track of who uses what so that I can likely figure out who's behind an attack because everyone leaves their own "clues" behind [171, 172]
- Overcome the students denial in underperforming. [130]

Proactive analysis / reviewing historical events

- Run queries automatically for me just to see if anythign comes back (aka, don't wait for me to have to do it) [40]
- Go back in time to review old alerts once new information/ data comes out to see if a breach happened that I may not have known occurred. [92]
- Monitor previous searches and findings to ensure they are still working as expected / reporting back to me [159]
- Periodically review entities that I may have looked into a while back (ie, look at historical events and see if theyr'e still occuring) [236]
- Search against my black list of IPs on a regular basis [237]

Understanding how / why

- Examine my data by asking why something may have happened. [264]
- Review previous logs in order to build a timeline around an incident [91, 189]
- Analyze existing collected information [10]
- Use historical trends/data to see if we've ever seen a similar event in the past [188]
- Create scenarios around incidents to better understand how/why those incidents occurred [218]
- Review data in excel file exports to gain greater clarity into the data [233]

Finding key insights

- Run queries against internal database to find new insights [18]
- Review IDS data from months ago to see if there were IoCs that I may have missed related to an incident I'm investigating [120]
- Look across any/all connections in order to find even small insight. [22]
- Look outside of the common places to find key insights like odd websites and traffic patterns [148]
- Review existing task repositories to see if we are already collecting something that might be useful [26]
- Find the very first time it showed up in my system even if its not directly talking to an IP addres [241]
- Keep queries that return no results because they may prove useful down the road (aka new intel comes in) [39]
- Correlate disparate data sets so that I don' tmiss key findings [271]
- Understand how the attacker thinks [354]
- Look through old logs for things I may not have even knew occurred [93]
- Utilize attacker methodology to leanr to be stealthy [353]
- Examine existing relationships to see if there are further relationships that ight not be obvious [21]
- When reviewing an alert, use details of that alert to look in new/unexpected areas using data like IP addresses or hosts. [106]
- Stay out of the areas where an operator or analyst would look [355]
- Use historical trends/data to see if we've ever seen a similar event in the past [188]

Key insights

★ CUSTOMIZE
The user needs to have flexible/useful tools to manage their daily workflow that align with how they want to work. Examples include being able to set individual priorities, personal alerts and track key data points.

★ CONTEXT
The user prefers to understand as much as possible around the “Why” with regard to their workflow and the details. This can come from the analyst, the “customer”, the software and the alerts themselves as long as they have the context required to understand the organizational goals.

★ COLLABORATE
Sharing/collaborating with colleagues is very important to the user in order to gain insights, save time and prevent duplication of efforts. This can happen at any point in the response cycle – before, during after – so long as it is occurring on a regular basis.

★ CONNECT
The user needs to be able to visualize relationships between people, places, and processes. They prefer software that allows them to do this themselves but also does it automatically provided it includes background / why into the connection.

Next steps

Near term
Explore the existing feature set and align those to concept areas.

Ensure the new UI and workflows align to how users think.

Create user journey / empathy maps that align with findings.

Future
Select areas to explore/brainstorm based on business goals, beyond first release.

Compare any new requests to MM to ensure the investment aligns with users’ asks.

Expand the MM to include differnet/new user segments.