Orange
Cyberdefense

Holistic Threat Modeling

An own Orange Cyberdefense threat informed defense approach for threat informed assessments and workshops to help customers improve their security postures.

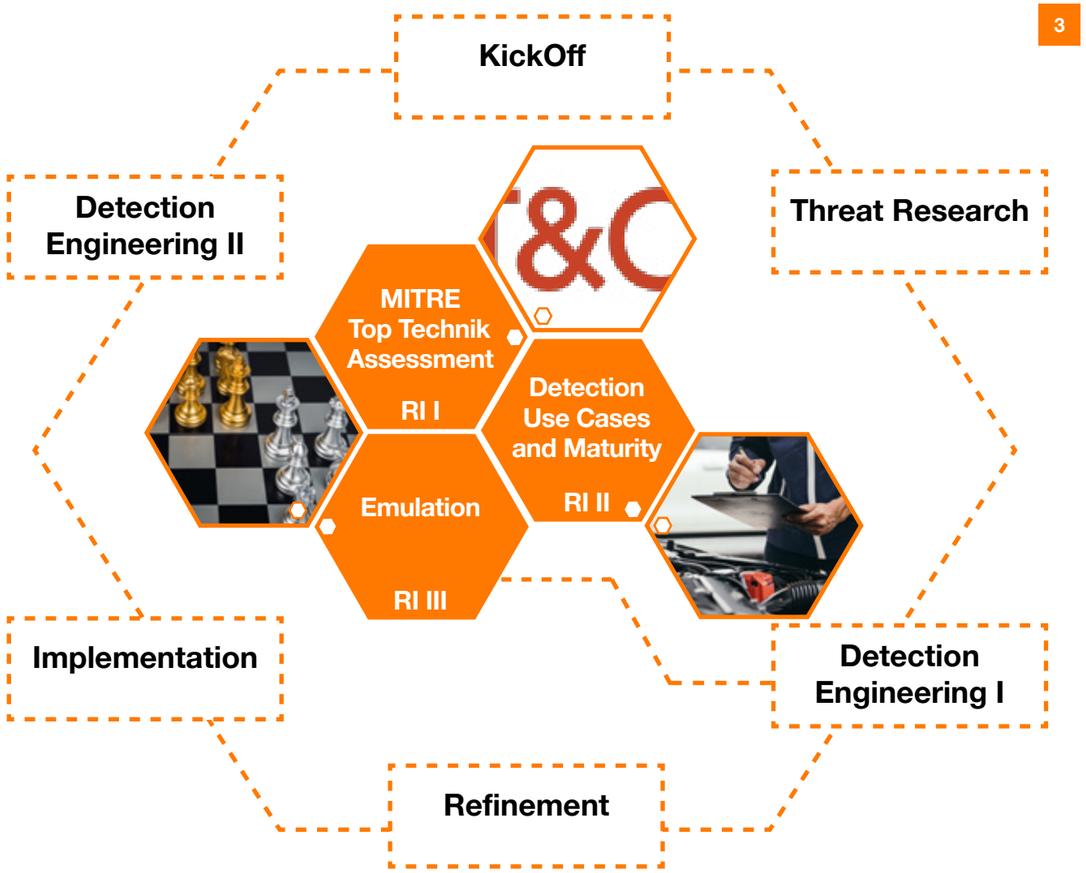
With the newly developed holistic threat modeling approach, Orange Cyberdefense shows how customers can daily analyze more effectively to improve their security posture and how we can provide them with our managed services and analysis.

Some Theory - Criteria for a Model and Assessment

There are many developed threat models and also many security frameworks, but what are the criteria for a specially developed threat modelling assessment so that it has the necessary characteristics to be suitable for a model?

For this purpose, the HSSEDI Institute defines the following criteria in the document Cyber Threat Modeling: Survey, Assessment, and Representative Framework:

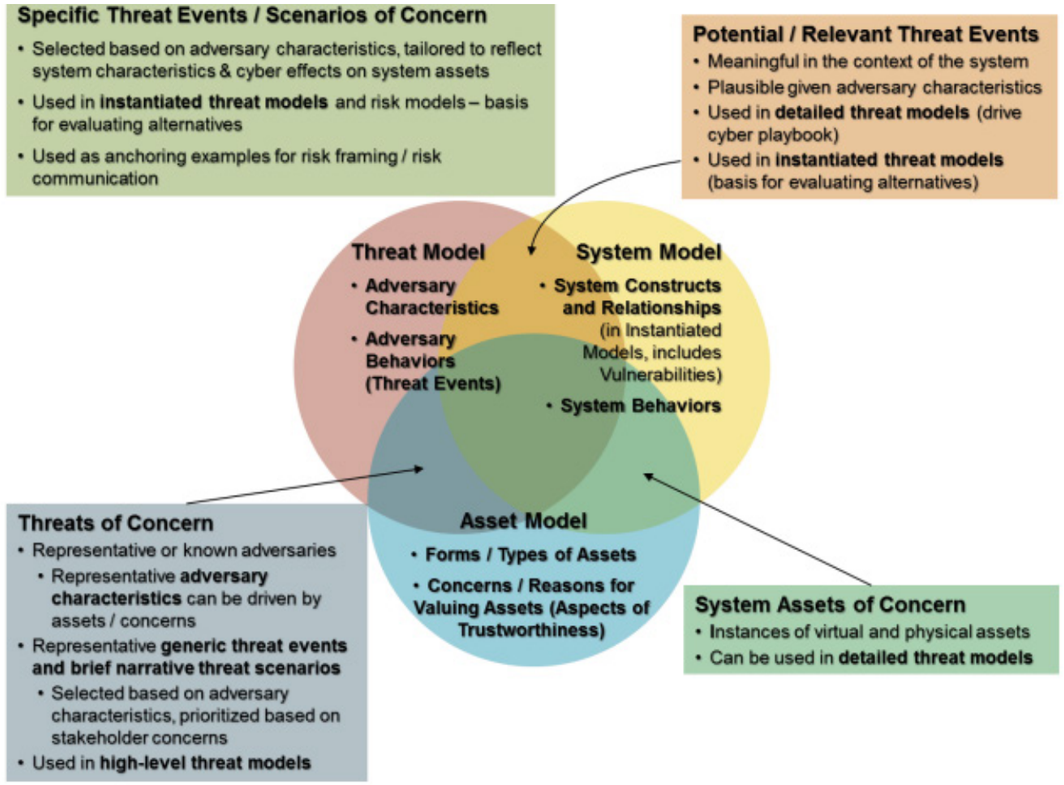
In the self-developed holistic threat modeling, we use the taxonomy of MITRE ATT&CK and D3FEND to be able to represent the relationships. Algorithms can be stored with automation, as many manufacturers are already doing today. However, this is not part and goal of the analysis with our model, but certainly feasible. With holistic threat modeling, we want to go into the analysis options of the analyst when one must deliver repeatable and reproducible results. The degree of detail and the granularity, complexity and rigor play a very important role. Knowing the data sources and telemetry is at least as important as the attack vectors. Testing something measurable, making it comparable, being agile while enabling transparency and identifying vulnerabilities is a challenge. This is where holistic threat modeling steps in.



The model tries to cover as many realistic attack scenarios as possible. As with other models, the possibilities are not endless. There are for example behavioral patterns that can be studied within the frameworks of ATT&CK or D3FEND but there is also always room for improvement. Certainly, there will always be more patterns and other opportunities for threat actors to attack customers' environments. Neither the holistic threat modeling nor the MITRE ATT&CK claim to be complete. It serves as a knowledge-based approach to find solutions and answers to given questions. Integrating further attacks is a challenge also in the future, but one can continue to develop own MITRE ATT&CK sub-techniques or D3FEND countermeasures using tools such as the MITRE ATT&CK and D3FEND- for e.g., valuable D3FEND artifacts to understand technical terms. In holistic threat modeling, the life cycles of cyber-attacks play at least as much a role as insider threats, attacks on supply chains, but NOT or less on non-cyber-attacks. The holistic view also includes Cyber Threat Intelligence, so the specific area of application, the business environment as well as the technical environment and threat environment are integrated. This can be worked out using specific questionnaires in the assessment. The latest scientific findings play just as important a role as daily reports of attacks, be it via threat intelligence reports, official institutions such as BSI or CISA or simply social media such as Twitter and news in the media. With holistic threat modeling, Orange Cyberdefense tries to be as specific as possible about the goals of the assessment and dive deep into the technical implementation. Through the repetitive iterative procedure, innovations are adapted, expanded, and further specified. Scalability is not only related to the aspect of coverage but also becomes important in defensive engagement when the corresponding detection needs to be tested. The more concrete the technical definition is, the more concrete are results in the emulation.

Threat models serve as input to risk modeling processes, giving the organization the visibility needed to implement countermeasure advances in a structured, repeatable, measurable, and rapid manner.

Threat Modeling Approaches



https://www.mitre.org/sites/default/files/2021-11/prs-18-1174-ngci-cyber-threat-modeling.pdf page 58

Reproducible and rapid improvement are keywords here, but so are visibility and counter-defense with successful prevention of attacks. In addition to Red Team and Blue Team, holistic threat modeling also supports Purple Teaming because it enables the holistic view that is necessary to combine incident response with forensics, detection engineering, CTI and a Red Team. Different perspectives make it possible to come back to one essential point, the common taxonomy of the MITRE ATT&CK and D3FEND. The assessment and model then enable the identification and evaluation of defense strategies. It shows which technologies are relevant, suggests test cases and scenarios, shows the effectiveness of the technologies, the progress of mitigation and prevention as well as detection, and refers to the possibilities of other approaches and frameworks like NIST or CIS.

Holistic Threat Modeling

With this self-developed form of threat modeling, we go into the implementation of holistic MITRE detection engineering using threat informed defense. The starting point is always the MITRE ATT&CK and the possibilities it offers to carry out gap analysis in addition to CTI regarding threats.

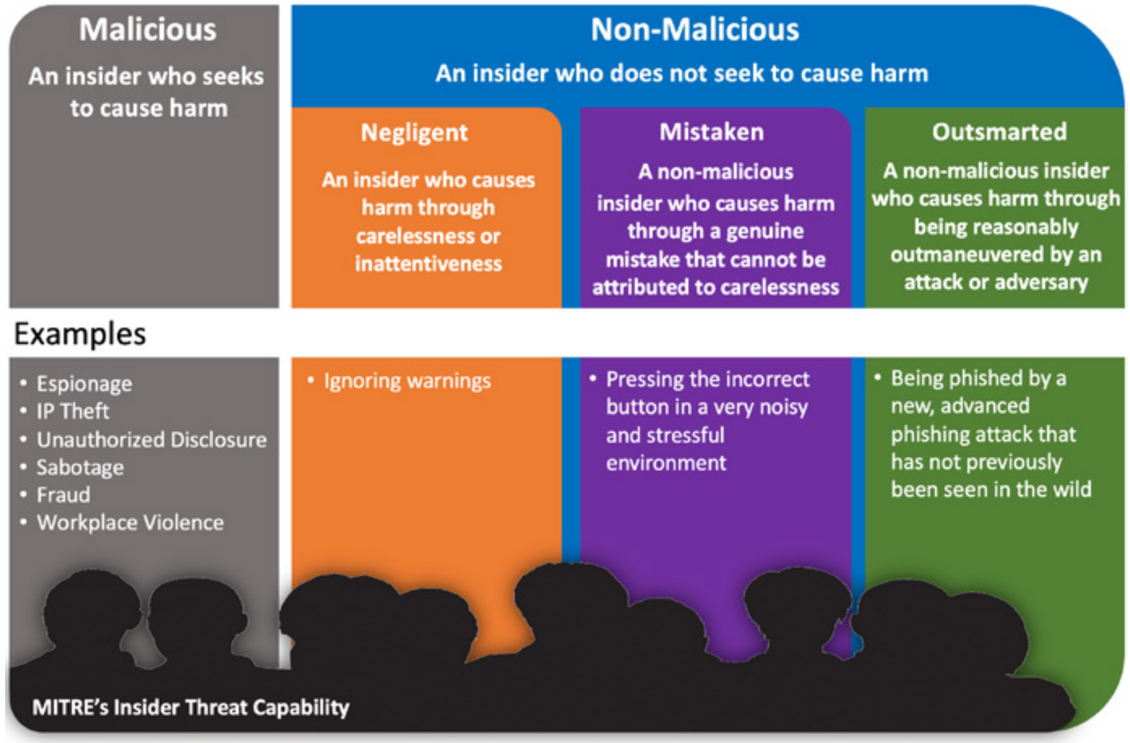
In addition to the actual threat intelligence and threat research, the focus is on integrating incident response, forensics (level 3 investigation and remediation) and proactive threat hunting into the detection engineering process. How can detection engineering lead to an improved incident response at the same time? To what extent can threat hunting contribute to an improved IR and how can forensics support this? Why is collaborative work so important here?

Collaboration & Sharing

In many companies, this is either only implemented in sub-areas or the departments work independently of one another. But how important a strategic orientation can be, becomes apparent in an emergency. This not only begins with the preparation of playbooks, but also ends with the efficiency, context, and speed of the incident response process, which also represents remediation at a deeper, forensics understanding during an investigation. Automation with breach and simulation tools like AttackIQ help to improve the readiness.

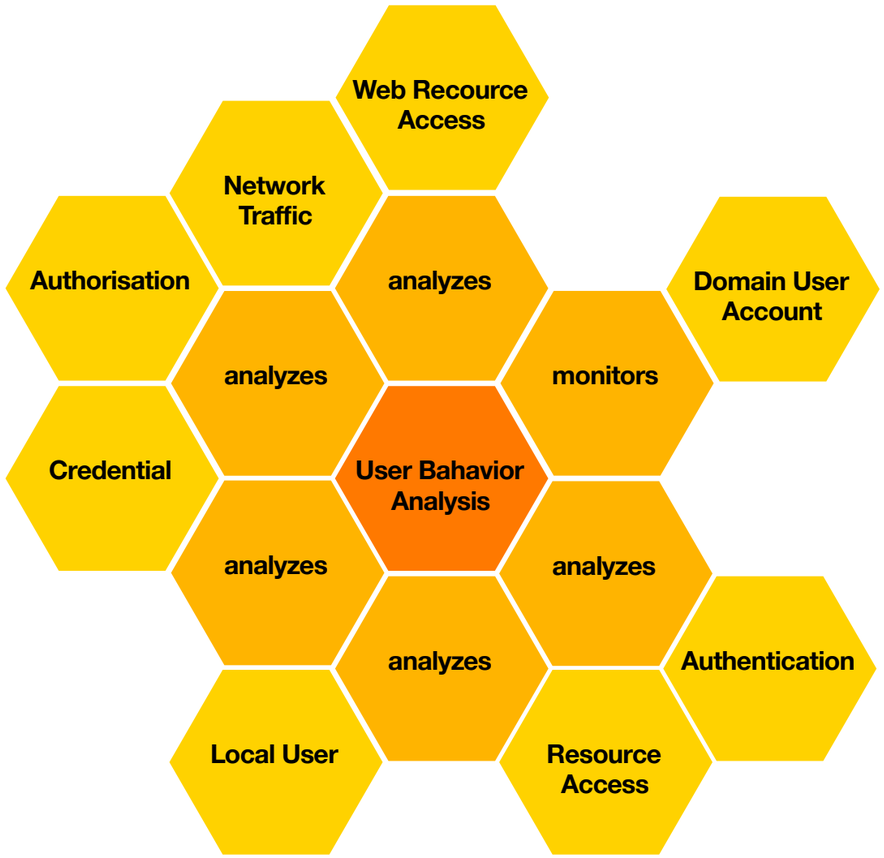
Automation and Semantics

The more detailed the understanding of the system landscape and the attackers is, but also of the threats posed by insider threats, the better and faster the actual incident response is. Automated breach & attack simulations play an equally important role when it comes to transparency and visibility of attacks and hardening through security controls. SOAR offers the possibility to map the MITRE ATT&CK and D3FEND automatically through ML and AI solutions. Insider threats can be determined via UEBA, and MITRE also offers approaches for the techniques to be considered here. The D3FEND presents this ontologically and helps to go deeper into the new technological concept or to understand existing systems. Language is used not only to understand technology but also to describe it intelligently.



MITRE's Human-Focused Insider Threat Types

D3FEND can help to understand User Behavior Analysis if an analyst tries to find malicious behavior or just want to study the countermeasure to improve the own environment.



Essential Components of Holistic Threat Modeling

Cyber Threat Intelligence, Defense Engagement as well as Collaboration & Sharing are essential components of holistic threat modeling. These aspects are considered in every phase of the assessment or the actual implementation.

Threat intelligence insights are important in incident response. They give the analyst the opportunity to understand attacks, but also to successfully recognize or defend against them. The same is especially true for MITRE Detection Engineering. During an IR or investigation process, threat hunting can then also be carried out with the help of a threat intelligence report. In the ideal case, IR, investigation, and threat hunting run hand in hand and the degree of automation is very high in a world-class SOC.

The Degree of Maturity

The degree of the maturity a company has regarding threat informed defense, decides which processes and procedures could be optimized with the threat model. Orange Cyberdefense defines together with you how progressive your people, processes, technologies, and detection posture in your company is. In some cases, such information is also unknown, if the maturity is rather low. In this case OCD would first start with an assessment that tries to define the goals, missions, internal and external threats. A more progressive or larger company has already done the preparatory work, has trustworthy service providers, its own analysts or assessments that have already been carried out. Here you can start with automation and proactive “elements” in detection or threat hunting.

CONCLUSION

The principle of holistic threat modeling is based on threat informed defense. It does not claim to cover all areas or to be an ultimate answer to all questions or attack vectors. However, it is an excellent opportunity to approach projects strategically and by means of rapid improvement. In addition to threat intelligence, the analyst not only tries to understand the attacks, but also to test them to see how new concepts, security controls or important assets and security solutions would withstand a specific threat actor or campaign. Tests can be specific to campaigns or security solutions, but also done for configurations and wherever technology can be analyzed with MITRE ATT&CK and D3FEND.