MaGMa: a framework and tool for use case management

1 Introduction

A Security Operations Center (SOC) has a central role in protecting against, and dealing with cyberattacks. In the ever changing landscape of cyber security, there are many threats to protect against. Each of these threats can have unique indicators in different parts of the cyber killchain [1]. It is the job of the SOC to recognize the cyber threats facing the organization in an early stage, mount the appropriate response and help to adjust security parameters to avoid breaches. This process of monitoring for manifestations of cyber threats is called security monitoring.

1.1 Security Monitoring

To support the security monitoring process, a security monitoring system is used. In particular, a SIEM (Security Information and Event Management) system is an essential part of the security monitoring processes. Additional monitoring systems, such as anomaly detection, intrusion detection (both network based and host-based) and big data platforms for analytics can also be found in more elaborate security monitoring infrastructures.

1.2 Security monitoring use cases

To provide a structured approach to security monitoring, use cases are used. Essentially, use cases describe manifestations of threats from a high level (the modus operandi of the cyber criminals) to the lowest level (concrete security events in the infrastructure such as exploits, failed logins, etc.). Use cases also describe follow-up actions (incident response) and are tied with business drivers to show how security monitoring reduces risk in the organization. Within the complexity of the security architecture, use cases can provide structure and overview.

1.3 MaGMa Use case framework

To organize use cases, a use case framework should be used. Such frameworks enable control over use cases and provide insight into identify how well an organization is capable of defending against cyber threats. For this purpose, the MaGMa Use Case Framework (hereafter called: MaGMa) was created in a collaborative effort of several financial institutions associated with the Dutch Financial Information Sharing and Analysis Community (FI-ISAC). MaGMa stands for Management, Growth and Metrics & assessment. MaGMa is based on the existing framework and tool developed and used by ABN AMRO Bank, complemented with views, experiences and best practices from other financial institutions. The framework consists of a document outlining the framework and a supporting tool for actual management of use cases within the SOC.

---

[1] http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

This article represents a brief version of the full MaGMa documentation. The full document and the tool can be obtained from:
https://www.betaalvereniging.nl/veiligheid/publiek-private-samenwerking/magma/

2 MaGMa use case definition and model

The focus group started off by creating the following definition for use cases:
"A use case is a security monitoring scenario that is aimed at the detection of manifestations of a cyber threat". A use case has a strategical, tactical and operational component.

With the definition in place, elements of the use case could be identified to create a use case model. The elements that comprise the use case be divided into three layers:

- Business layer. The business layer of the use case describes how the use case is connected to the organization's business needs.
- Threat layer. The threat layer of the use case describes the threat that the use case is intended for. Several aspects of the threat are important.
- Implementation layer. This is the operational layer, where aspects that are relevant for implementation of the use case in the operational security monitoring architecture are described.

These layers were discussed in detail, which led to the following use case model:

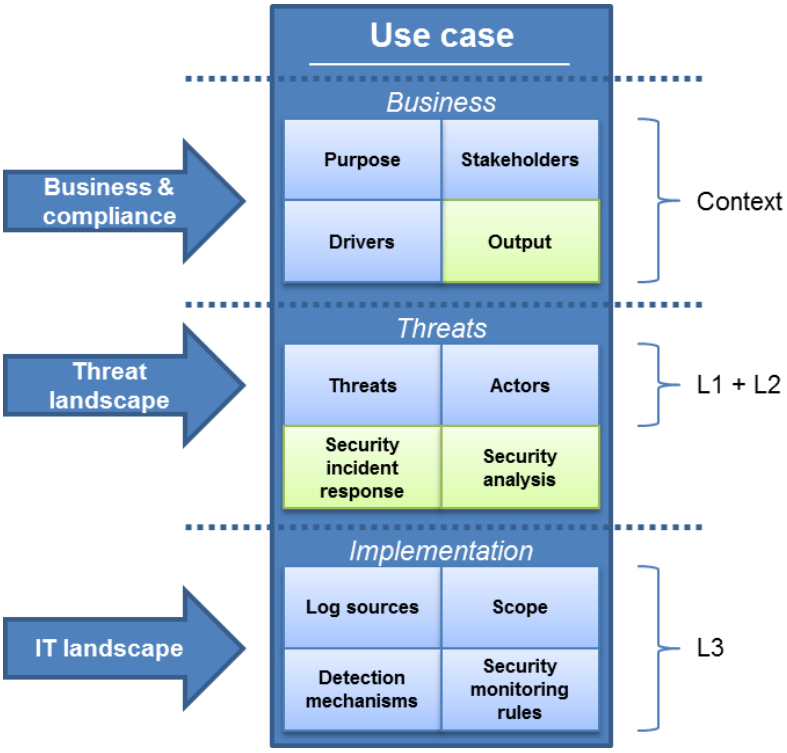

Figure 1: Use case model

The blocks in blue color can also be found in the supporting MaGMa UCF tool, the green blocks are part of the use case, but documented elsewhere in the security monitoring documentation.

3 MaGMa elements

With the use case model in place, the basis for MaGMa was created. Each of the elements (Management, Growth and Metrics & assessment) will be explained hereafter.

3.1 Management of Use Cases

When the use case framework has been created, it also needs to be maintained. This is what use case management is for. Essentially, it is life cycle management for use cases. And is built-up out of 4 phases: onboarding, operational, maintenance and offloading.

3.1.1 Onboarding (plan and build)

For the onboarding of new use cases, the use case elements from the model should be made concrete. Stakeholders that provide input into the use case must be made part of the process to ensure proper alignment with these stakeholders. Once all relevant information has been identified, the use case can be documented and operationalized.

3.1.2 Operational phase (run)

In the run phase of a use case, all operational elements are implemented and running as part of daily security operations. Concretely, this means that:

- Log sources have been added to the security monitoring systems and supplying the required information.
- Scope has been determined and implemented for this use case
- Security incident response is known and documented
- Roles and responsibilities for this use case have been formally documented
- Security monitoring rules have been implemented, tested and documented

3.1.3 Maintenance (change)

There are several types of input that lead to changes within the use case. Most likely, these changes will be carried out at the implementation level, although changes at the threat and business levels will occasionally be required. This section identifies potential sources for input into change management for use cases. These can be divided into 2 main drivers:

1. Environmental drivers. These are changes to use cases resulting from changes in the organization. Environmental drivers include changes to the threat landscape, changes to the business, changes in rules and regulations and changes in the IT infrastructure.
2. Operational drivers. Additionally, operational drivers can lead to change as well. Red team testing as incidental input for improvement and lessons learned from

incident response as a continuous input for improvement are important to consider. Threat hunting is also an important driver for change.

3.1.4 Offloading (decommission)

When use cases are no longer required, an offloading process should be followed to remove the use case from the framework at each of the layers. The same inputs that feed the change management of the use case may trigger the decommissioning of the use case.

Figure 2 provides an overview of the life cycle management process and the input received.

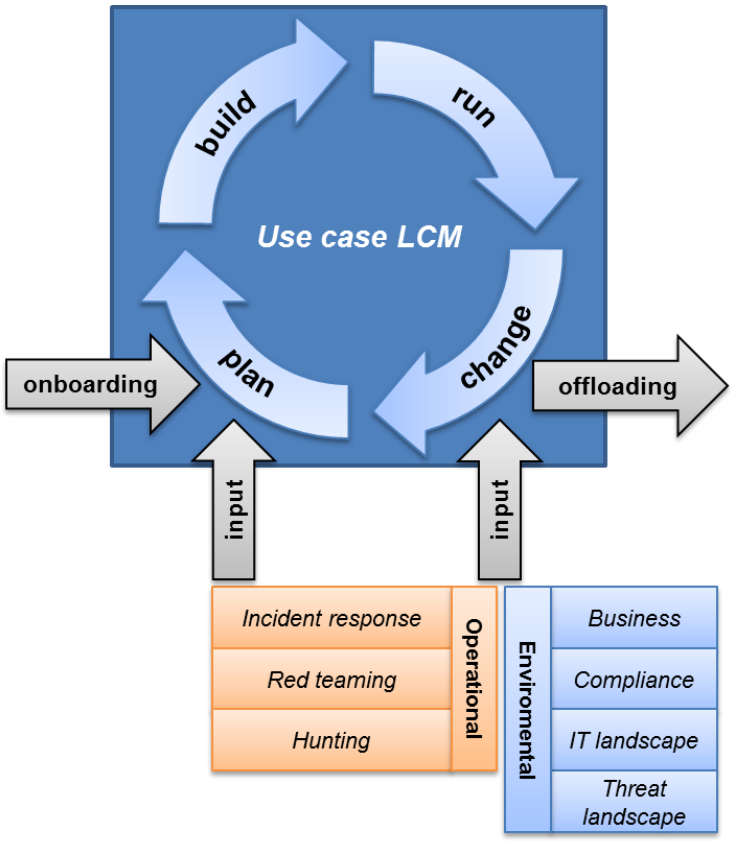

Figure 2: Use case management overview

3.2 Growth (Capability and Maturity)

With a use case framework in place and several use cases implemented, an important question arises: how to move towards more mature and more effective security monitoring? To answer this question, 2 aspects must be evaluated. These aspects are capability and maturity.

3.2.1 Capability

Use case capability deals with how well a SOC is capable of detecting security threats. Highly capable SOCs will have multiple layers of detection (detection-in-depth) and advanced security tooling for security monitoring. Of course, these SOCs also have highly professional

personnel to ensure that their advanced technical capability is backed with equally advanced analyst knowledge.

Growing in use case capability can be done by growing the number of use cases (framework completeness), or by increasing the quality of an existing use case (use case completeness). This can be by increasing the number of assets (log sources), by adding new types of assets to the security monitoring systems or increasing the number of security monitoring rules.

The most effective risk-based approach to capability growth is by first using risk levels to identify high-risk use cases and then using residual risk to determine the required implementation level per use case before moving to the next use case.

3.2.2 Maturity

Maturity deals with how well a SOC is able to provide effective security monitoring continuously and how well it can adequately deal with the output of security monitoring. A highly mature SOC will provide consistent and repeatable output in terms of high-quality reports and effective incident response. Additionally, a highly mature SOC will improve continuously and consistently through a standardized process. Therefore, standardization and documentation are significant aspects of maturity.

According to the CMMI [2], the 5 maturity levels can be identified:

1. Initial: ad-hoc and chaotic operations.
2. Managed: structured security monitoring.
3. Defined: fully structured use case framework.
4. Quantitatively Managed: goals are set for quality in the use case management process.
5. Optimizing: characterized by continuous improvement.

3.3 Metrics & Assessment

To determine the effectiveness of the use case framework in delivering optimal security monitoring, metrics are required. The MaGMa framework should be regularly assessed using these metrics. The outcome of such assessments can be used to identify strong and weak spots within the framework. Note that the focus here is on quantifiable metrics. Three types of metrics have been identified: embedded metrics, control metrics and output metrics. Each of these types will be examined.

3.3.1 MaGMa UCF embedded metrics

There are several metrics embedded into the UCF. These metrics are used to provide steering information regarding the effectiveness of the use case framework. The embedded

[2] http://cmmiinstitute.com/

metrics include effectiveness, implementation level and coverage. From these values weight and potential are calculated. Weight is the overall score of effectiveness, implementation and coverage; potential provides insight into the growth potential of the use case by calculating weight relative to effectiveness.

3.3.2 MaGMa control metrics

Control metrics provide governance information on the framework itself. The control metrics that can be used are: changes to the framework, growth in number of use cases: measure change in monitoring scope, growth in weight and changes to potential.

3.3.3 MaGMa output metrics

The last category of metrics is metrics on the output of the MaGMa framework. The following metrics were identified are: the number of alerts, number of incidents per use case, false-positive ratio and number of false-negatives. False-positives indicate quality and efficiency, while false-negatives indicate gaps in security monitoring.

4 MaGMa tool

The MaGMa UCF tool supports the use case management process. The tool contains all elements of the use case model depicted as blue blocks in figure 1.

4.1 Tool layers

On the right-hand side of figure 1, the phrases L1, L2 and L3 are used. These represent the three layers of the use case as they are used in the MaGMa tool:

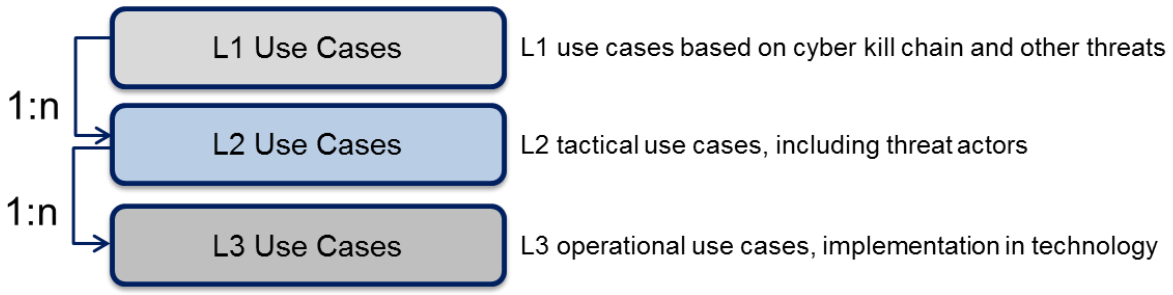

Figure 3: Use case layers and relation

Each of these layers addresses different elements of the use case. At the L3 layer, a technical use case at the operational level is described. At the L2 and L1 layer, use cases are described at a tactical level and connected to threat actors, business drivers and compliance drivers.

4.2 Tool usage

Usage of the tool is explained in detail in the tool itself, but the basic steps for implementation are the following:

1. First, outline the strategical business layer. This will provide the necessary context for the concrete use cases. Outlining the business layer is done by speaking with

business stakeholders and determining purpose, business drivers and optionally compliance drivers for the framework.

2. Then, create the L1 use cases using the threat landscape. The 7 basic L1 use cases representing the steps in the cyber kill, complemented with 6 additional L1 use cases are already present in the tool. Additional L1 use cases that are specific for your industry should be added. For example: financial fraud (for the financial sector), Industrial control system sabotage (for energy and utilities sector).
3. Once the L1 use cases have been finalized, L2 use cases can be put into place. An extensive list of 62 L2 use cases is already present in the tool. This list was created using input from all participating organizations. The list may contain use cases that are not applicable to your organization, or may not fully cover your security monitoring requirements. Therefore, it is important to carefully select the proper use cases and extend upon this list where required and useful. Note that for steps 2 and 3, it is of vital importance to include security management stakeholders to ensure proper alignment with organizational risk & security management processes.
4. Lastly, the L3 use cases should be outlined and operationalized. First, outline all of the actual L3 monitoring rules. Then fill in all other applicable operational elements (log sources, scope and detection mechanisms) for each of the L3 rules as desired. Furthermore, the embedded metrics as described in chapter 5 should be set for each of these rules when they are operationalized. A number of L3 rules are already present in the tool, based on the MITRE ATT&CK Matrix for Enterprise [3].

The MaGMa UCF tool can be used to setup a new monitoring environment or can be easily integrated into an existing environment.

5 Conclusion

Use case management is an essential activity in any mature SOC. The use case management process allows the SOC to gain control over a large and growing number of use cases by structuring the use cases, connecting them to business and compliance drivers and threats. The MaGMa framework was designed specifically to support the use case management process. The tool provides a very practical and flexible approach to managing use cases in any security monitoring environment, from simple to complex. In total, 12 L1 use cases, 62 L2 use cases and 169 L3 use cases have been predefined in the tool, giving organizations a jumpstart in use case management.

MaGMa UCF works to be in control over your security monitoring process and aligning the security monitoring to business and compliance needs. The framework provides the ability to prove to your stakeholders that the SOC is in control and adequately managing and decreasing risk in the enterprise.

[3] https://attack.mitre.org/

Authors
Rob van Os, de Volksbank, *lead author and UCF developer*
Floris Ladan, ABN AMRO Bank, *UCF lead developer*
Thomas van Casteren, Rabobank, *UCF developer*
Robin Toornstra, Euroclear
Robert Metsemakers, Achmea
Lambrecht Nieuwenhuize, BNG Bank
Holger Grotenhuis, Triodos Bank

Additional contributions by
Kelvin Rorive, Rabobank
Marcus Bakker, ING Bank
Tony Tromp, ABN AMRO Bank, *UCF developer*