MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS

Milestone Security Development Lifecycle (SDL)

milestone

Contents

Milestone Security Development Lifecycle (SDL)

This document describes the Security Development Lifecycle for Milestone Systems A/S (hereafter referred to as Milestone).

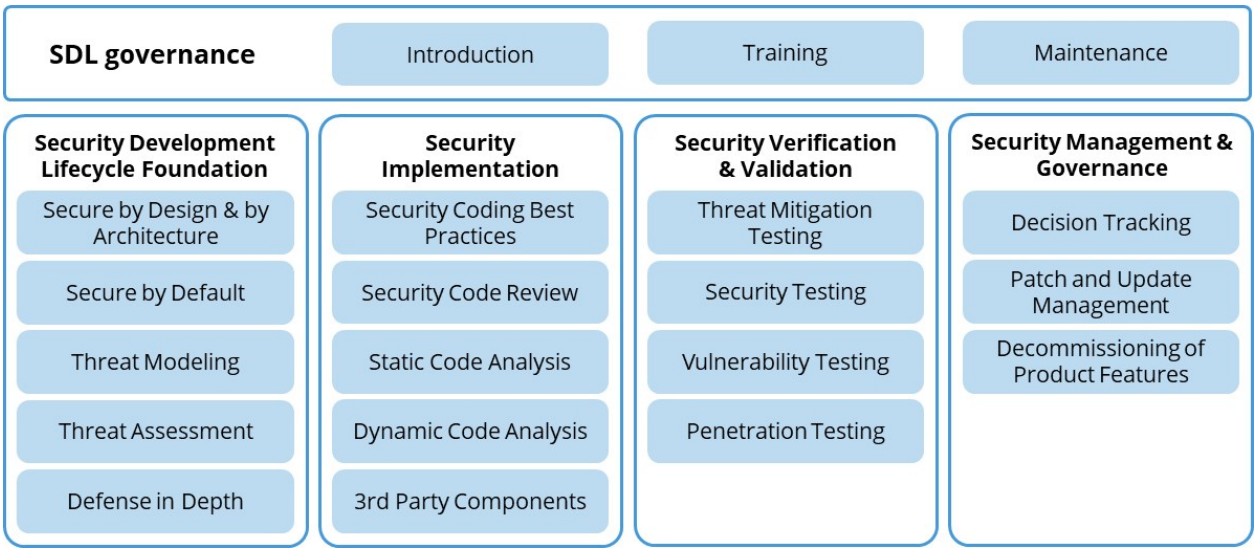
The Security Development Lifecycle (SDL) encompasses a comprehensive set of principles and practices that extend beyond the software-coding activities and pure technical aspects of our products.

Scope

Milestone's SDL encompasses the broader context of our development processes, and defines the requirements, practices, and procedures, that Milestone employees follow during development of all Milestone software products and services.

In addition to focusing on reducing the attack surface and safeguard against vulnerabilities in Milestone's software products, the SDL also focuses on compliance with industry standards and regulatory requirements, resulting in safer products, services and systems.

The following sections describe the areas covered by the SDL as illustrated below.



SDL Implementation

Milestone's SDL is implemented throughout Milestone's Technology Group, through a continuous process, where everyone initially has received an introduction to and training in the processes and procedures the SDL describes. After the initial introduction and training, the knowledge and application of the SDL is maintained though the following activities:

- new employees attend internal 'Milestone Developer Academy' training, which covers training in Milestone's development process and tools, training in our SDL and finally XProtect product training.
- through Milestone's "security champions" program for the development teams, the 'Security and Compliance' team will continuously work with the security champions, to ensure they remain proficient in the processes and procedures described in our SDL.
- when the SDL is updated to a degree that is deemed to require additional training, the development teams and security champions are informed of the changes and receive training in the changes.

Note: Security champions are team members in each development team that have taken on an additional role to function as an extension to the "Security and Compliance" team. The security champion works as the team's local security expert and link to the "Security and Compliance" team.

Review process

Milestone reviews this SDL yearly and updates it to follow the latest changes in industry standards, emerging threats, new technologies, and organizational policies.

SDL owner

The Milestone Security Development Lifecycle is owned and maintained by Milestone's 'Security & Compliance' team.

Secure Development Lifecycle Foundation

Security isn't a feature. It's a core principle that supports Milestone's development process.

In this section, the fundamental secure requirements are described. They ensure that every product, tool, or service Milestone releases is shielded as best possible against potential threats and vulnerabilities.

The secure requirements cover essential procedures and criteria such as threat modeling, secure coding practices, and vulnerability tests and assessments. Each requirement has been carefully crafted to bolster the defense of Milestone's products, tools, and services to protect both our customers and their users against cybersecurity threats as best possible.

Secure by Design and Secure Architecture

"Secure by Design" and "Secure Architecture" are closely related concepts in the field of cybersecurity and software development. They both emphasize the proactive incorporation of security principles into the design and development processes to create robust, resilient, and less vulnerable software products.

Secure by Design
Secure by design is a holistic approach to software development where security considerations are integrated into the entire software development lifecycle, from the initial design phase to deployment and maintenance. It places a strong emphasis on foundational security principles, such as the principle of least privilege, input validation, and secure coding practices.

The primary goal of secure by design is to address security at the earliest stages of development to prevent security vulnerabilities and weaknesses from being introduced in the first place.

Secure Architecture
Secure architecture is a part of the broader secure by design philosophy. It focuses on designing the overall structure and components of a system to be inherently secure, considering the system's intended functions and potential security risks.

Specifically, secure architecture refers to the structural design of a system, software application or service and the network communication between system components. A secure architecture encompasses the design decisions that ensure data confidentiality, integrity, and availability, in addition to access control, secure communication, and other security-related aspects.

The relation between Secure Architecture and Secure by Design
The relation between secure architecture and secure by design lies in their shared objective of building secure and resilient systems from the ground up. In summary, secure architecture is a fundamental component of the broader secure by design approach. It involves designing the structural and architectural aspects of a system with security in mind, aligning with the principles and philosophy of Secure by Design to create robust and resilient software products.

Milestone will, during the design and development of Milestone's products, tools and services, adhere to the concepts of Secure Architecture and Secure by Design as described here.

Secure by default

Milestone implements our software according to the secure by default principle, which is a principle in software development that aims to design and implement software systems with the highest level of security from the outset. This means that when a software product or system is deployed, it is by default configured to provide the strongest possible protection achievable without user configuration, minimizing potential security risks.

Secure by default covers the following areas, which Milestone will ensure to adhere to.

Default settings
Milestone's software is developed to provide secure default settings to ensure our software offer the best protection against common security threats.

Least privilege
Milestone's software is developed to adhere to the principle of least privilege.
This specifically means that software components interacting with other components of the Milestone products, are implemented with only the privileges necessary to perform the component's intended tasks in the overall product.

This principle of least privilege also applies to user management, where, by default, new "standalone" users or roles containing multiple users, have no permissions until deliberately assigned permissions by the administrator of the software or system.

Authentication and authorization
Milestone's software is developed to always provide strong authentication mechanisms that is enforced to access the software or system. Additionally, Milestone's software will always provide authorization functionality to ensure users and integrated components or systems only can access resources they specifically have been granted access to.

Secure communication and encryption
Milestone's software is, by default, developed to provide or use secure encryption for data at rest and during transmission. For functions where user configuration is needed to enable encryption, Milestone's software is developed to request the user to perform the required configuration, or alternatively choose to disable encryption.

Explicit change consent
Milestone's software is designed to not make any changes to the host computer's operating system or it's security settings that might reduce the security without detailed explanation to the user and the end-user's explicit consent.

Optional functionality off by default
Milestone's software is designed to reduce the cybersecurity attack surface and to reduce personal information exposure. This is done by having features, functions, services, or use of external services that are not critical for the fundamental functionality of the software, disabled by default.

Customers can then enable this functionality when needed. In cases where it is deemed that the user must be informed of the potential consequences of using the functionality, the user is informed about this, so the choice to enable it is an informed decision.

Fail securely
Milestone's software is designed to follow the "fail securely" principle. One example of this principle is user authorization for accessing a resource. Only in the case where all parts involved in validating the user's access permissions works and passes checks is the user provided access to the resource. In case a component fails, so access permissions cannot be checked or a security token cannot be renewed, access is denied.

Open design
Milestone's software is designed to follow the "open design" security principle. This principle dictates that security may not rely on secrecy of the implementation. Instead, with "open design" the implementation, protocols, security measures and so on are publicly documented and can be examined and reviewed by anyone without this compromising the security and safeguards of the software.

Threat modeling

Threat modeling is a systematic approach used in software development to identify, evaluate, and mitigate potential security threats and vulnerabilities. It involves defining the security requirements, analyzing the software system's design and architecture, identifying how attackers might exploit weaknesses and compromise its security and then mitigate the threats and validate that they have been mitigated.

Threat modeling is not a one-time activity, but an iterative process that continuously is performed when new functionality is implemented, or major changes are made.

By performing continuous threat modeling, development teams can effectively identify potential security issues early on, leading to a more secure and robust software product. Additionally, integrating threat modeling into the development process ensures that security is not an afterthought but a fundamental consideration throughout the entire software development lifecycle.

Threat assessment

As described in the Threat Modeling process, Milestone's development teams will perform threat assessments at various stages throughout the software development lifecycle, to ensure the security of the developed components, features, or changes made.

Initial design and planning (Define):
Threat assessment activities are initiated during the initial requirements definition, design, and planning phase of the software development process. By incorporating threat assessment and security considerations early on, it is easier to identify potential risks and security requirements, leading to the development of a secure design.

Pre-development (Diagram):
Before the development phase begins, a threat assessment must be conducted to review the proposed architecture, technologies used, and security controls that are to be implemented. This assessment helps identify any major vulnerabilities or design flaws that need to be addressed before development starts.

Development (Identify and Mitigate):
Throughout the development process, Milestone's development teams conduct regular threat assessments, typically in the form of code reviews, to identify potential security vulnerabilities in the code and address them.

Integration and Testing (Validate):
As components, features, or changes are integrated into the software product, a threat assessment is carried out to ensure the security of the integrated system. This threat assessment involves vulnerability scanning, penetration testing, and other security testing techniques to identify vulnerabilities and weaknesses in the system.

Repeated threat assessment cycle

Prior to Release:
Before releasing Milestone software to customers, a final threat assessment is conducted to verify that all identified vulnerabilities have been addressed and that the software meets the required security standards. This assessment may involve additional penetration testing, vulnerability scanning, or security audits.

Ongoing Maintenance and Updates:
Threat assessments are not limited to the development and deployment phases. Regular threat assessments are conducted during maintenance and update cycles of the Milestone software. This ensures that any new vulnerabilities that may have been introduced through updates or changes are identified and mitigated promptly.

Periodic and Regulatory Assessments:
In extension to the threat assessments performed during the development phases, Milestone conducts periodic threat assessments to ensure and maintain the security of the software product over time – even when nothing has been changed.

The reason for this is that new threats might appear after the software initially was developed and threat assessed. This periodic threat assessment might include scheduled vulnerability scans, penetration testing, and compliance assessments to ensure adherence to current security standards and regulatory requirements.

Defense in depth

Defense in depth is a security principle where several layers of security safeguards and risk-mitigation countermeasures are implemented. With such security layering, if one defense layer fails, another layer is there to block an attack. This intentional redundancy creates greater security and can protect against a wider variety of attacks.

Milestone implements our software following the defense in depth principle, to ensure that our customers can implement multiple security layers to protect their Milestone installation.

The list below shows a non-exhaustive list that exemplifies this principle applied in Milestone's software:

- Support for standard IT- and network-security measures, such as VLAN, VPN, firewalls, virus scanners and more
- Encryption of data in transit and at rest
- Support for various user authentication methods, including external identity providers (IDPs) offering multi-factor authentication and other security functionality
- Detailed permission control and enforcement
- Role separation between IT administration and security administration and operation.

Secure implementation

Secure implementation is not a one-time task. It's a mindset. This mindset runs through every stage of Milestone's development process. It means that Milestone's development teams proactively work on identifying and addressing security vulnerabilities, follow best practices, and adhere to established guidelines to ensure the resilience of Milestone's products – both in terms of software and hardware products.

The following guidelines cover requirements for secure implementation. The guidelines include security coding best practices, security code review, static and dynamic code analysis, and security policies for third-party components. By adhering to these guidelines, Milestone's developers reduce the risk of security vulnerabilities, ensure safeguard of user data, and uphold Milestone's commitment to be a trusted and reliability vendor.

Security coding best practices

Milestone has defined a *Security Coding Best Practices* standard, which defines the practices and rules all Milestone developers are trained to and must follow during development of our software products.

The *Security Coding Best Practices* govern the way Milestone's code must be written, reviewed, and maintained to ensure our products remains resilient against security threats. The standard address areas with potential vulnerabilities and guide developers in crafting robust software to face cybersecurity challenges.

While the *Security Coding Best Practices* standard provides practices and rules that, by default, must be followed, Milestone recognize that certain products, features or tools might have unique requirements and/or priorities. In these special cases, additional documentation defining the practices used for the special case must be created and approved by the Milestone's Security and Compliance Team.

Security code review

Security code review is an essential part of Milestone's development process. Its purpose is to identify potential vulnerabilities and security weaknesses in the software's source code, to validate adherence to our *Security Coding Best Practice standard,* to ensure that the implementation aligns with the secure coding requirements, and to enhance the overall security posture of our software.

To ensure consistent code review, Milestone has defined a set of *Security Code Review Guidelines* which reviewers must follow when they perform code reviews.

Static code analysis

The purpose of static code analysis is to automatically analyze the source code for potential vulnerabilities, bugs, and adherence to defined coding standards. Milestone incorporates static code analysis in our software development process to proactively identify issues early in the development process. This ensures that new issues are detected and fixed before they reach our customers in a product release.

When a warning over the defined threshold is found, it is fixed with a traceable solution. The solution can either be changes to the code or if the warning is a false-positive, it can be muted. In case the warning is muted the development teams responsible for the code must document why this warning is a false-positive.

Third-party components

Third-party components include libraries, frameworks, plugins, and other external software used in Milestone's software to provide functionality, security features, and enhance efficiency.

Integrating existing third-party components can significantly increase speed of development and add features and security functionality that adheres to approved standards to the Milestone software products and services. However, when using third-party components, it's crucial to be aware of the potential security risks associated with using these components, because they can have significant impact on the overall security of Milestone's software.

To ensure third-party components adhere to Milestone's security requirements and standards, a security assessment will be performed for every third-party component Milestone intends to use. The security assessment aims to identify known vulnerabilities, security history, and the responsiveness of the vendor to security issues.

Approved and verified third-party components that are allowed to be used in Milestone's products and services are stored in a Milestone-controlled repository. Milestone will monitor the allowed third-party components for updates and security patches to ensure the latest secure version are used.

Milestone regularly scans Milestone's application and its dependencies, including the third-party components used, for known vulnerabilities using appropriate security tools.

The penetration testing Milestone regularly performs on our products and services also covers functionality introduced by third-party components to identify potential vulnerabilities introduced by the third-party components.

Milestone will produce a SBOM report in a standard format covering all used third-party dependencies for every software version released.

Security verification and validation

This section covers the essential processes of security review, verification, and validation done by Milestone's development teams during all phases of our product development.

These processes are crucial to:

- Detect manually identifiable vulnerabilities in critical components:
- Understand application resilience from a black-box perspective:

Selective manual security testing

Milestone's approach to security testing includes selective manual testing, complemented by a combination of static and dynamic tools. This combination guides and focuses our review to specific areas of the application, approaching them as an attacker would. While we also use automated tools, which are effective in uncovering various vulnerabilities, the automatic tools can never replace the expertise of a trained human reviewer.

Prioritizing high-risk modules

Recognizing that vulnerabilities in security-critical parts of our XProtect software products can have a substantial impact for our customers, integrators and partners, our development teams prioritize the security review of high-risk modules. These modules often include critical functionality such as authentication mechanisms, access control enforcement points, session management schemes, external interfaces and APIs, and input validator/data parsers.

Strategic combination of metrics and automated scans

To determine the best areas for scrutiny, our development teams uses a blend of code-level metrics and focused automated scans. This approach enables our developers to channel their efforts effectively. The security review process may take on various forms, including pair programming, peer review, time-boxed security focus phases involving the entire development team.

Threat mitigation testing

Milestone performs threat mitigation testing to verify how effective the implemented mitigations address the identified threats. The threat mitigation testing aims to:

- Validate that the implemented threat mitigation solution is effective and provides the expected level of protection.
- Attempt to bypass or defeat the implemented threat mitigation solution to evaluate its resilience against further modified attacks.
- Assess the overall security robustness against potential attacks in the product area of the implemented threat mitigation.

Milestone will also maintain a detailed record of the threat mitigation testing performed. The record documents who performed the test, when it was done, which fixed vulnerability was tested, the result of the test, as well as any new vulnerabilities, weaknesses, or deviations from expected results that are found.

Security testing

The primary objective of security testing is to assess the effectiveness of the implemented security controls and identify any potential vulnerabilities that malicious actors could exploit. Security testing also helps ensuring that the components, features, or changes comply with the required security controls and practices.

Each development team in Milestone has the ownership of a set of components and/or supplementing services and tools. Following best practices, each development team performs security tests for the components, services, and tools they are responsible for developing and maintaining. In addition to the testing done by the development teams, the security and compliance team also runs time-boxed internal pen-testing to supplement the security testing before each release.

Security testing is an ongoing process, and the scope evolve as the system changes or new threats emerge. For this reason, each development team are held responsible for maintaining a proactive and adaptive approach to security throughout the development lifecycle of the components they are responsible for.

Security testing performed by Milestone's development teams covers the following areas and techniques:

- Identifying assets
- Analyzing threat landscape
- Defining security requirements
- Prioritize critical functionality
- Documenting scope
- Perform periodic reviews
- Adopt security standards and best practices
- Automated and manual testing
- Documenting results

Vulnerability testing

Milestone conducts vulnerability testing for all new features, functions, APIs, and interfaces implemented to identify and characterize potential security vulnerabilities in the product. This includes weaknesses, misconfigurations, and design flaws that attackers could exploit.

Vulnerability testing covers the following areas and techniques:

- Abuse case and, malformed-input testing
- Attack surface analysis
- Known vulnerability scanning
- Software composition analysis
- Dynamic runtime resource management testing

Milestone also maintains a detailed record of the vulnerability testing performed. The record documents who performed the test, when it was done, the product/version/feature/interface tested, any identified vulnerabilities, their impact, and any recommended actions. It also documents the testing techniques and tools used, and any specific configuration used during the testing.

Penetration testing

With the purpose of identifying potential vulnerabilities and security weaknesses in our products, and to ensure that our software product meets current security standards and can withstand real-world attacks, Milestone conducts penetration testing for every XProtect VMS product version released.

For all other XProtect software products and Husky products, penetration testing is done on-demand or as per the predefined schedule based on the products criticality and risk level.

Performing regular penetration testing allows Milestone to proactively identify and address potential security vulnerabilities before our software are deployed in customer installations.

The penetration testing is performed by skilled and certified penetration testers, and aims to:

- Identify vulnerabilities and security weaknesses in the product
- Validate the effectiveness of the implemented security controls and defenses
- Assess the resilience of the product against various attack vectors
- Provide actionable recommendations to improve the security posture of the product.

In addition, Milestone maintains a detailed record of each penetration testing performed. The record documents who performed the test, when it was done, the product and version tested, the result of the test, as well as the remediation decisions and actions taken including result of retesting remediations.

Security Management & Governance

Milestone's commitment to security extends beyond the initial development phase. It covers every facet of the software lifecycle, ensuring that security is not a mere afterthought but a continuous, integrated process throughout the software's lifecycle.

Milestone recognizes that security incidents can occur despite our best efforts. For this reason, we have a Vulnerability Management Policy with which Milestone commits to promptly address and mitigate internally and externally reported security breaches when they are reported.

Also as a CVE Numbering Authority (CNA) under the MITRE domain, Milestone follows industry best practices in managing and responding to security vulnerabilities discovered in our products.

Decision tracking

To document and track the decisions made during the software development process, Milestone will keep a record of the decisions made and the reasons for those decisions, for the following software development areas:

- Design and architecture decisions
- Requirements and exceptions
- Technologies used
- Use of third-party components and/or integrations.

Patch and Update Management

During the product's lifetime, Milestone will provide customers with on-demand software patches to address identified security vulnerabilities and critical bugs.

With each software patch, Milestone provides information on:

- What vulnerabilities or bugs are being addressed
- How important it is to apply the patch
- Clear and precise instructions on how to apply the software patch

Milestone will also, at regular intervals, release new versions of our products to enhance functionality, security, and improve user experience.

The patch and update management process empowers customers to independently safeguard their systems and data by installing security patches and updated versions as soon as they are available, allowing the customers to keep their installation current and secure.

Decommissioning of product functionality

As our software evolves, certain features, interfaces or APIs may outlive their usefulness, critical vulnerabilities may be identified that cannot be mitigated without extensive redesign, or the functionality, implementation, or technology used are simply deemed insecure by current standards.

When this happens, Milestone initiates a process to decommission the functionality to minimize potential security vulnerabilities and maintain the overall integrity of our software.

When functionality is being decommissioned, Milestone will announce it in the release prior to the release where the functionality will be decommissioned. This means that it typically is announced at least four months before the functionality is decommissioned, which will provide customers and partners time to plan for a transition and make necessary arrangements.

When functionality is decommissioned, Milestone will provide recommendations and guidelines, on how to address the changes. This may involve upgrading to a newer version of the software, migrating to a different Milestone product, or exploring third-party options.

In case the decommissioned functionality store user data, Milestone will provide guidelines or tools to assist users in safely migrating their data or exporting the data to a usable format.

helpfeedback@milestone.dk

About Milestone

Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone Systems enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone Systems is a stand-alone company in the Canon Group. For more information, visit https://www.milestonesys.com/.