kaspersky

Bosch IP video surveillance camera platforms: Security Maturity Assessment Report

#2021-0009-0002-EXT

Kaspersky ICS CERT

27.09.2021

kaspersky

About the Security Maturity Assessment 3
Overview 3
Object of assessment 3
The goal of the Security Maturity Assessment 4
The method for the Security Maturity Assessment 5
Security Maturity Target 6
Security maturity assessment results 7
Security Program Management 9
Compliance management 10
Threat modeling 11
Risk attitude 12
Product supply chain risk management 13
Services third-party dependencies management 14
Establishing and maintaining identities 15
Access control 16
Asset, change and configuration management 17
Physical protection 18
Protection model and policy for data 19
Implementation of data protection controls 20
Vulnerability assessment 21
Patch management 22
Monitoring 23
Situational awareness and information sharing 24
Event detection and response plan 25
Remediation and recovery and continuity of operations 26

kaspersky

About the Security Maturity Assessment

Overview

The following is the security maturity assessment public report for Bosch IP video surveillance camera platforms.

The assessment is based on the IIC IoT Security Maturity Model (IoT Security Maturity Model, IoT SMM) developed by the Industry IoT Consortium (IIC). The assessment also takes into consideration the Security Maturity Target, which was developed earlier for this platform.

The report is prepared by Kaspersky ICS CERT.

Object of assessment

The following IP cameras are considered as an object of assessment:

- **FLEXIDOME IP starlight 8000i - 8MP (*NDE-8504-R*)**
- **FLEXIDOME IP micro 3000i (*NDV-3502-F03*)**

The following IP cameras were supplied for the vulnerability analysis conducted as a part of security maturity assessment:

- **FLEXIDOME IP starlight 8000i - 8MP (*NDE-8504-R*)**
- **FLEXIDOME IP micro 3000i (*NDV-3502-F03*)**

Based on their similar functionality, firmware developed for the cameras, and processes implemented to support security capabilities, the results of this security maturity assessment can be applied to the following cameras:

CPP14

1. FLEXIDOME multi 7000i
2. FLEXIDOME panoramic 5100i

CPP13

1. AUTODOME inteox 7000i
2. MIC inteox 7100i

CPP7.3

1. AUTODOME IP 4000i
2. AUTODOME IP 5000i
3. AUTODOME IP starlight 5000i (IR)
4. AUTODOME IP starlight 7000i
5. DINION IP 3000i
6. DINION IP bullet 4000i

7. DINION IP bullet 5000
8. DINION IP bullet 5000i
9. DINION IP bullet 6000i
10. FLEXIDOME IP 3000i
11. FLEXIDOME IP 4000i
12. FLEXIDOME IP 5000i
13. FLEXIDOME IP starlight 5000i (IR)
14. FLEXIDOME IP starlight 8000i
15. MIC IP starlight 7000i
16. MIC IP starlight 7100i
17. MIC IP ultra 7100i
18. MIC IP fusion 9000i

CPP7

1. DINION IP starlight 6000
2. DINION IP starlight 7000
3. DINION IP thermal 8000
4. FLEXIDOME IP starlight 6000
5. FLEXIDOME IP starlight 7000
6. DINION IP thermal 9000 RM

CPP6

1. AVIOTEC IP starlight 8000
2. DINION IP starlight 8000 12MP
3. DINION IP ultra 8000 12MP

Results of vulnerability analysis conducted as a part of the overall assessment may be not fully applicable to the cameras from this list.

The goal of the Security Maturity Assessment

IP video products are becoming commonplace in today's network environment. And as with any IP device on a network, the protection of the network against attacks also depends on the device's features and security capabilities. There is no one-size-fits-all video security solution. Different situations call for security capabilities of the camera.

However, the vendor wants to confirm that the existing security capabilities of devices provide a secure enough basis for the long-term assurance that the devices do not pose significant concerns regarding data and video security, or the overall protection of the networked environment where the camera is installed.

The goal of this Security Maturity Assessment and enhancement is to support the effective, and not arbitrary, use of mechanisms. The approach aligns the comprehensiveness (degree of depth, consistency and assurance of security measures) and scope (degree of adherence to industry or system needs) of security needs with investments in appropriate practices.

The purpose of the Security Maturity Assessment is to evaluate the maturity of the security practices implemented in device development, use and maintenance

processes. This maturity is represented by two indicators: comprehensiveness and scope. The target levels of these indicators are documented by the Security Maturity Target developed for the device.

The Security Maturity Target establishes the ultimate security maturity state for a given system. The target includes a consistent set of security practices, providing all stakeholders an understanding of the general security goals and purpose of each security practice.

The method for the Security Maturity Assessment

The assessment of the current security maturity state was conducted on the basis of Bosch employee interviews, security and customer documentation analysis, and IP camera vulnerability research results.

Interviews were conducted in two stages:

- The first stage was based on the completed questionnaire with questions not linked to concrete security practices to avoid imposing desired levels of comprehensiveness
- The second stage came after processing the results of the first stage. At this stage, the preliminary results of comprehensiveness evaluation were provided. Then an additional questionnaire was used to address inconsistencies in the first stage, close the gaps and request the necessary evidences to support answers wherever necessary. Practice scope (general, industry or system) was also assessed at this stage.

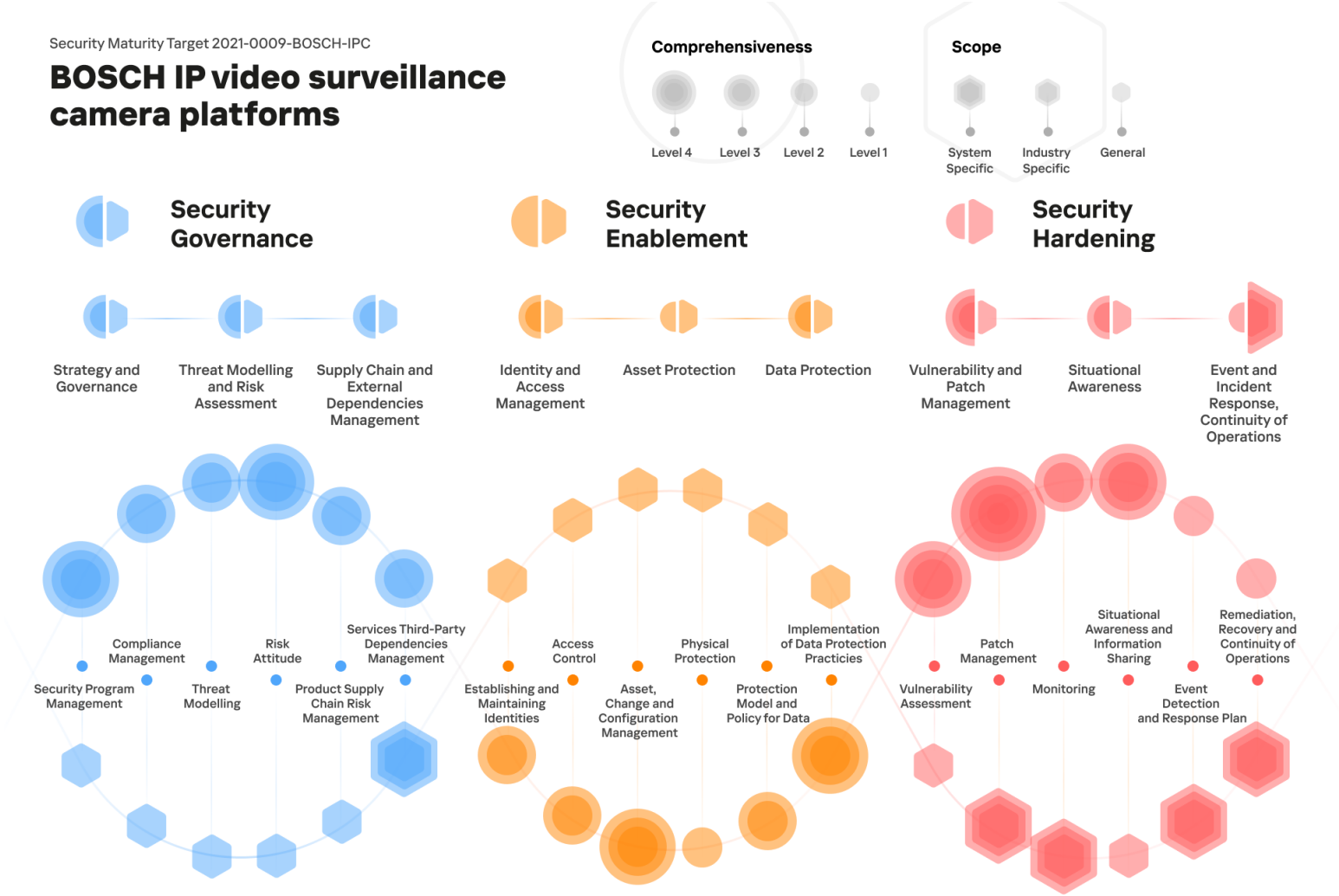
Vulnerability assessment conducted as the separate and independent activity provided the information on the following aspects:

- How the declared comprehensiveness level of practices related to the Security Enablement domain correspond to the actual technical implementation of such practices. Vulnerabilities that were found and appropriately addressed helped confirm comprehensiveness as concerns the technical implementation of appropriate security measures
- How the declared comprehensiveness level of practices related to the Security Hardening domain, especially Vulnerability Assessment and Patch Management, correspond to the actual processes applied to deal with vulnerabilities and patches. Actions undertaken by the Bosch team helped confirm as concerns the appropriate processes.

Interview results and the analysis of evidence, security and customer documentation, and the report on IP camera vulnerabilities research (provided here as an Appendix #1, Vulnerability Research Report #2021-0009-0002-VR) lead to conclusions about the conformance of assessment subjects to the declared Security Maturity Target.

kaspersky

Security Maturity Target



kaspersky

Security maturity assessment results

Practice	Target Comprehensiveness	Current Comprehensiveness	Target Scope	Current Scope
Security program management	3 / Consistent	3 / Consistent	General	General
Compliance management	2 / Ad hoc	2+ / Ad hoc	General	General
Threat modeling	2 / Ad hoc	2+ / Ad hoc	General	General
Risk attitude	3 / Consistent	3 / Consistent	General	General
Product supply chain risk management	2 / Ad hoc	2 / Ad hoc	General	General
Services third-party dependencies management	2 / Ad hoc	2 / Ad hoc	System	System
Establishing and maintaining identities	2 / Ad hoc	2 / Ad hoc	General	General
Access control	2 / Ad hoc	2 / Ad hoc	General	General

Asset, change and configuration management	3 / Consistent	3 / Consistent	General	General
Physical protection	1 / Minimum	1 / Minimum	General	General
Protection model and policy for data	2 / Ad hoc	2 / Ad hoc	General	General
Implementation of data protection practices	3 / Consistent	3 / Consistent	General	General
Vulnerability assessment	3 / Consistent	3 / Consistent	General	General
Patch management	4 / Formalized	4 / Formalized	System	System
Monitoring	2 / Ad hoc	2 / Ad hoc	System	System
Situational awareness and information sharing	3 / Consistent	3 / Consistent	General	General
An event detection and response plan	1 / Minimum	1 / Minimum	System	System
Supporting remediation, recovery, and continuity of operations	1 / Minimum	1 / Minimum	System	System

Security Program Management

Comprehensiveness and Scope levels	
	3 / Consistent **General**
Objective	
	Bosch aims to create a security program aligned with its organizational structure and systems.
Conclusion	
	Practice implementation represents actions based on the desired plan and the creation of the appropriate organization. **Security Program Management is in line with comprehensiveness level 3 / Consistent.** **The scope of practices is General.**

kaspersky

Compliance management

Comprehensiveness and Scope Levels	
	2 / Ad hoc **General**
Objective	
	Bosch aims to analyze and understand compliance requirements for implementation.
Conclusion	
	Company practices demonstrate an understanding of the compliance requirements and the ability to perform assessments or outsource them. **Compliance Management is in line with comprehensiveness level 2+ / Ad hoc.** **The scope of practices is General.**

kaspersky

Threat modeling

Comprehensiveness and Scope Levels	
	2 / Ad hoc **General**
Objective	
	Bosch aims to perform vulnerability analysis to identify threats. Address is in an ad-hoc manner.
Conclusion	
	Company practices involve vulnerability assessments to understand threats as they pertain to the camera. Recognized methods and specific tools are used for threat modeling. **Threat Modeling is in line with comprehensiveness level 2+ / Ad hoc.** **The scope of practices is General.**

kaspersky

Risk attitude

Comprehensiveness and Scope Levels	
	3 / Consistent **General**
Objective	
	Bosch aims to establish procedures for detailed risk assessment and differentiates the importance of risks.
Conclusion	
	The risk is well understood but managed in an ad-hoc manner. **Risk attitude is in line with comprehensiveness level 3 / Consistent.** **The scope of practices is General.**

kaspersky

Product supply chain risk management

Comprehensiveness and Scope Levels	
	2 / Ad hoc **General**
Objective	
	Bosch aims to implement analysis, contracts and methods for reviewing and protecting the supply chain.
Conclusion	
	Product supply chain ad-hoc analysis and methods are used to track security measures undertaken by suppliers and the effectiveness of these measures. **Product supply chain risk management is in line with comprehensiveness level 2 / Ad hoc.** **The scope of the practice is General.**

kaspersky

Services third-party dependencies management

Comprehensiveness and Scope Levels	
	2 / Ad hoc **System**
Objective	
	Bosch aims to provide service quality with service-level agreements and progress metrics in contracts. **Bosch adds specific goals to the definition of criteria. Specifically, device availability must be supported even in the event of external service failure. This changes the scope of this practice to System.**
Conclusion	
	Third-party service dependencies management checks that conformance to agreements is tracked, and that service-level agreements (SLAs) and progress metrics (e.g. KPIs, etc.) are defined. The proper work of the device is guaranteed even if external services are unavailable. **Third-party services dependencies management is in line with comprehensiveness level 2 / Ad hoc.** **The scope of the practice is System.**

kaspersky

Establishing and maintaining identities

Comprehensiveness and Scope Levels	
	2 / Ad hoc **General**
Objective	
	Bosch aims to achieve dynamic device identity.
Conclusion	
	The cameras can be identified. Role-based identities support access control to the device. **Establishing and maintaining identities is in line with comprehensiveness level 2 / Ad hoc.** **The scope of the practice is General.**

kaspersky

Access control

Comprehensiveness and Scope levels	
	2 / Ad hoc **General**
Objective	
	Bosch aims to restrict the ability of both internal and external agents to access devices and IT components.
Conclusion	
	Access controls consider both internal and external threats. Vulnerabilities in the access control mechanisms found during the assessment have been appropriately addressed. Role-based access control is available to align restrictions with anticipated scenarios of IP camera use. **Access control is in line with comprehensiveness level 2 / Ad hoc.** **The scope of the practice is General.**

Asset, change and configuration management

Comprehensiveness and Scope Levels	
	3 / Consistent **General**
Objective	
	Bosch aims to manage IT and OT assets in an integrated manner.
Conclusion	
	The management of camera configuration is implemented in a holistic and integrated manner. **Asset, change and configuration management is in line with comprehensiveness level 3 / Consistent.** **The scope of the practice is General.**

kaspersky

Physical protection

Comprehensiveness and Scope Levels	
	1 / Minimum **General**
Objective	
	Bosch aims to restrict access to physical assets in general.
Conclusion	
	As regards physical protection, Bosch does not provide much because the cameras should be installed by trained professionals only with a decent knowledge of how to set up a surveillance system and the physical protection required. **Physical protection is in line with comprehensiveness level 1 / Minimum.** **The scope of the practice is General.**

kaspersky

Protection model and policy for data

Comprehensiveness and Scope Levels	
	2 / Ad hoc **General**
Objective	
	Bosch aims to develop data classification systems in discrete environments.
Conclusion	
	Data is classified according to its business and security impacts, but the classification of different types of data is siloed. **The security model and policy for data is in line with comprehensiveness level 2 / Ad hoc.** **The scope of the practice is General.**

Implementation of data protection controls

Comprehensiveness and Scope Levels	
	3 / Consistent **General**
Objective	
	Bosch aims to implement systematic data protection measures across the entire system.
Conclusion	
	The sensitive data on cameras and transferred from/to cameras is protected across the entire system via multiple mechanisms at different layers. This protection is automated by well-recognized technical means. **Data protection control is in line with comprehensiveness level 3 / Consistent.** **The scope of the practice is General.**

Vulnerability assessment

Comprehensiveness and Scope Levels	
	3 / Consistent **General**
Objective	
	Bosch aims to perform holistic vulnerability analysis of the system as a whole using automation and third-party evaluations.
Conclusion	
	Bosch‘s vulnerability assessment practice meets the need for improved protection of critical components against cybercriminals with an intermediate skill level and insider attacks. **Data protection controls are in line with comprehensiveness level 3 / Consistent.** **The scope of the practice is General.**

kaspersky

Patch management

Comprehensiveness and Scope Levels	
	4 / Formalized **System**
Objective	
	Bosch aims to protect components with a long lifecycle and those are not easily patched due to certification or operational requirements.
Conclusion	
	Bosch has established a centralized patch management process for its IT and development environment. Automated patch management tools are provided for Customer devices connected to the Remote Portal. Firmware updates and patches are also available in the Download Store. Measures and workarounds in security advisories could be considered by customers as a way of improving their protection policy for obsolete devices and devices that are not easily patched due to operational requirements. **Patch management is in line with comprehensiveness level 4 / Formalized.** **The scope of the practice is System.**

Monitoring

Comprehensiveness and Scope Levels	
	2 / Ad hoc **System**
Objective	
	Bosch aims to obtain status events from devices and check for correct expected operation.
Conclusion	
	Implemented security monitoring spans events generated by individual components, devices, sensors and systems to detect security issues. Users can implement a centralized approach to monitoring. Malware is not detected because it is recognized as not relevant to the device (no malware has ever been discovered for the proprietary operating system, but this does not mean it cannot exist). A specific approach may be applied to keep the device working as long as possible without affecting it by diagnostic activities (system emulation). This narrows the scope of the practice to System. **Implementation of monitoring is in line with comprehensiveness level 2 / Ad hoc.** **The scope of the practice is System.**

kaspersky

Situational awareness and information sharing

Comprehensiveness and Scope Levels	
	3 / Consistent **General**
Objective	
	Bosch aims to have a general awareness of external incidents and implement a policy of sharing information with external parties on a need-to-know basis.
Conclusion	
	The implementation of this practice helps Bosch learn information about external incidents in a systematic manner. Information sharing policy supports responsible disclosure. **Situational awareness and information sharing practice is in line with comprehensiveness level 3 / Consistent.** **The scope of the practice is General.**

kaspersky

Event detection and response plan

Comprehensiveness and Scope Levels	
	1 / Minimum **General**
Objective	
	Bosch aims to provide guidance on how to detect and respond to incidents that can impact critical components.
Conclusion	
	This practice supports the sharing of zero-day vulnerabilities and is applicable if security assessments and testing activities are implemented. **The event detection and response plan is in line with comprehensiveness level 1 / Minimum.** **The scope of the practice is System.**

kaspersky

Remediation and recovery and continuity of operations

Comprehensiveness and Scope Levels	
	1 / Minimal **System**
Objective	
	Bosch aims to provide basic instructions for the system recovery.
Conclusion	
	Bosch defines the concrete minimalistic actions for the remediation and recovery of the camera. **Remediation, and recovery and continuity of operations practice is in line with comprehensiveness level 1 / Minimum.** **The scope of the practice is System.**

www.kaspersky.com

https://ics-cert.kaspersky.com