Bosch IP video surveillance camera platforms

Security Maturity Target 2021-0009-BOSCH-IPC

Kaspersky ICS CERT

27.09.2021

Contents

Overview

The purpose of this document is to describe the security maturity target for the Bosch IP video surveillance camera platforms prior to any external assessment of security features, their comprehensiveness and appropriateness for this type of device, and any further enhancement of these features.

Security Maturity Model approach and benefits

Not all systems and organizations require the same strength of protection mechanisms and procedures to be deemed secure enough. Organizations set the priorities that drive the security enhancement process, making it possible for the mechanisms and procedures to fit the organization's goals without going beyond what is necessary. The implementation of security mechanisms and processes are considered mature if they are effective in addressing those goals.

Reasonable security

Industry IoT Consortium

The Industry IoT Consortium is the world's leading organization transforming business and society by accelerating the industrial internet of things (IIoT).

Our mission is to deliver transformative business value to organizations, industry and society by accelerating adoption of a trustworthy internet of things.

The Industry IoT Consortium is a program of the Object Management Group®, Inc. (OMG®)

For more information,
visit www.iiconsortium.org

There is no silver bullet that can address security needs for every system. Organizations have differing needs, and different systems need different strengths of protection mechanisms. The same technology can be applied in different ways and to different degrees, depending on the needs.

It is the security mechanisms' appropriateness in addressing the goals, rather than their objective strength, that determines the security maturity. Hence, security maturity is the degree of confidence that the current security state meets all organizational security needs and all organizational security-related requirements. Security level, on the other hand, is a measure of confidence that system vulnerabilities are addressed appropriately and that the system functions in an intended manner.

Deciding where to focus limited security resources is a challenge for most organizations given the complexity of a constantly changing security landscape. Any rigorous security assessment procedure needs a scoring and prioritization method to evaluate the current state and development of a metrics-based security strategy. The goal of the Security Maturity Model (SMM) is to provide a path for internet of things (IoT) providers to know where they need to be and how to invest in security mechanisms that meet their requirements without over-investing in unnecessary security mechanisms.

Security Maturity Model

The Security Maturity Model (SMM) of the Industry IoT Consortium defines the levels of security maturity for an organization to achieve based on its security goals and objectives, as well as its appetite for risk. This enables decision makers to invest in only those security mechanisms that meet their specific requirements.

The purpose of the Security Maturity Model (IIC IoT Security Maturity Model, IoT SMM) is to determine the priorities that drive their security enhancements and the maturity required to achieve them.

The model fosters effective and productive collaboration among business and technical stakeholders. Business decision makers, business risk managers and owners of IoT systems, concerned about the proper strategy for implementing mature security practices, can collaborate with analysts, architects, developers, system integrators and other stakeholders responsible for the technical implementation.

Hierarchy of Security Maturity Practices

The core of the Security Maturity Model is represented by the hierarchy of the security practices. Figure 1 illustrates the structure of the SMM and the breakdown of security maturity domains. Domains are the high-level views that capture the key aspects of security maturity: governance, enablement and hardening. Each of the domains has different key aspects to it, called subdomains. For example, the hardening domain includes subdomains vulnerability and patch management, situational awareness and event and incident response. Each domain may use a variety of practices, both technical and organizational, to achieve results related to that domain.

This hierarchical approach enables the maturity and gap analysis to be viewed at different levels of detail, from the various domains overall to the individual practices.

Domains are pivotal to determining the priorities of security maturity enhancement at the strategic level. At the domains level, the stakeholder determines the priorities of the direction in improving security.

Subdomains reflect the basic means of obtaining these priorities at the planning level. At the sub domains level, the stakeholder identifies the typical needs for addressing security concerns.

Practices define typical activities associated with sub domains and identified at the tactical level. At the practices level, the stakeholder considers the purpose of specific security activities.

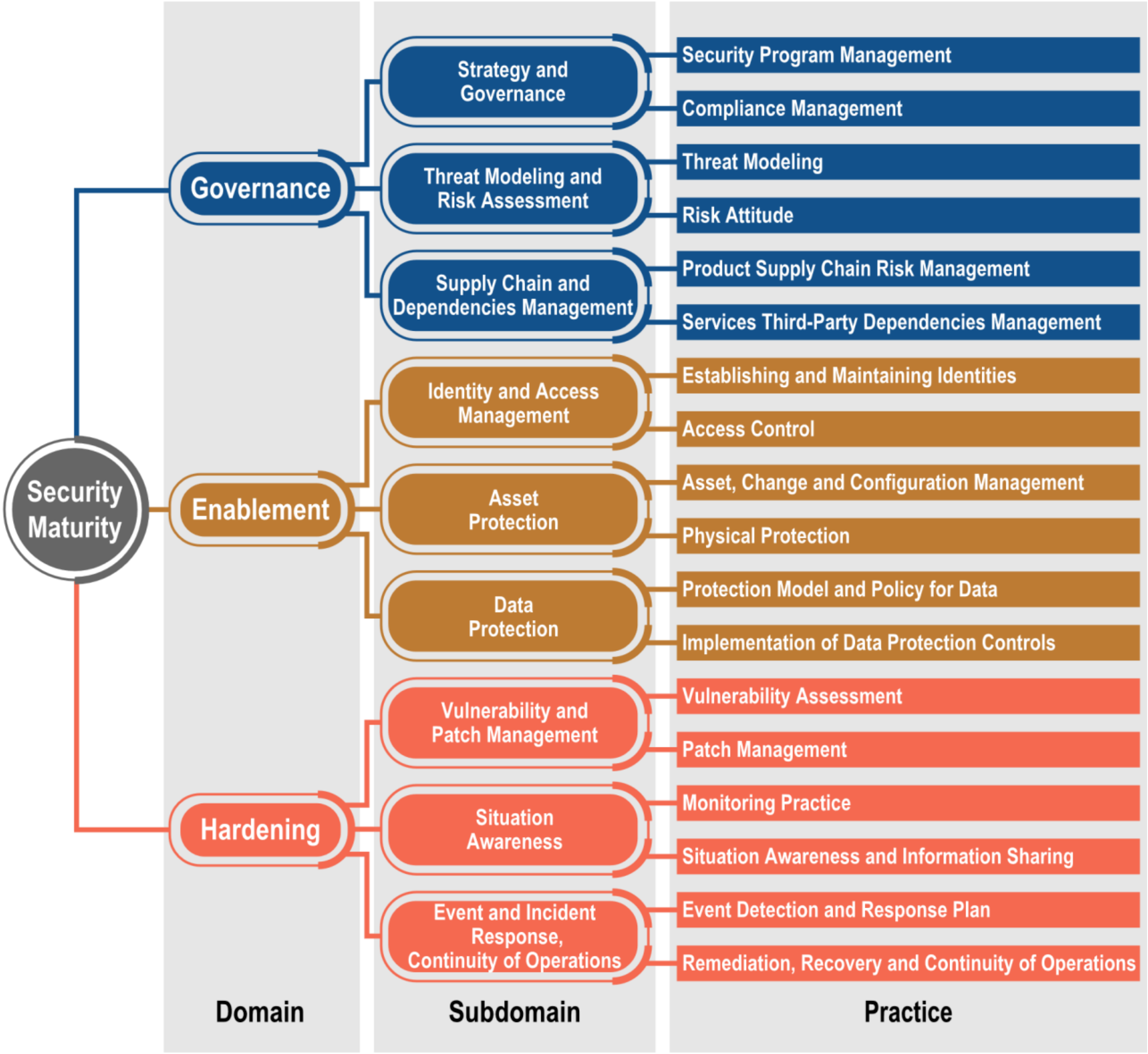

Security Maturity
Governance
Enablement
Hardening
Strategy and Governance
Threat Modeling and Risk Assessment
Supply Chain and Dependencies Management
Identity and Access Management
Asset Protection
Data Protection
Vulnerability and Patch Management
Situation Awareness
Event and Incident Response, Continuity of Operations
Security Program Management
Compliance Management
Threat Modeling
Risk Attitude
Product Supply Chain Risk Management
Services Third-Party Dependencies Management
Establishing and Maintaining Identities
Access Control
Asset, Change and Configuration Management
Physical Protection
Protection Model and Policy for Data
Implementation of Data Protection Controls
Vulnerability Assessment
Patch Management
Monitoring Practice
Situation Awareness and Information Sharing
Event Detection and Response Plan
Remediation, Recovery and Continuity of Operations
Domain
Subdomain
Practice

Figure 1 – IoT Security Maturity Model Hierarchy

Security Maturity Target

This section summarizes the analysis results according to device-specific factors described below as a part of the analysis. It represents the Security Maturity Target at each of the three levels: security maturity domains, subdomains, and practices. The process of establishing the levels is described in the next section.

The goal for Security Maturity assessment and enhancement is to support the effectiveness, not the arbitrary use of mechanisms. The approach aligns the comprehensiveness (degree of depth, consistency and assurance of security measures) and scope (degree of fit to the industry or system needs) of security needs with the investment in appropriate practices.

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 the purpose of each security practice.

Object of assessment and context of its use

The goal for this project is to assess and improve the security of the Bosch IP video surveillance camera platforms.

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

At the same time, the vendor wants to confirm that the existing security capabilities for every device provide the enough basis for the long-term assurance that the device does not pose significant concerns regarding data and video security.

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

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

Based on the similarities of the functional purpose, firmware developed for the cameras and processes implemented to support security capabilities, the following cameras may fit results of this assessment:

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

Factors to Consider in the Case Study System Analysis

Coverage. Bosch has built a solid reputation as a top provider of complete video surveillance solutions, be they basic or complex. Bosch's wide-ranging product lines include wired and wireless IP cameras, PTZ cameras, AutoDomes, video encoders, DVRs, NVRs and much more. One of the company's specialties is providing users with the necessary tools to integrate existing cameras into new, more advanced network surveillance systems. With advanced encoders and products, Bosch delivers the means to build sophisticated, flexible, and easily expandable video surveillance installations. All these factors make coverage quite wide and the scope where IP cameras can be applied quite diverse.

Exposure. The vectors for compromising IP cameras are easy to identify: via the internet, via the video surveillance infrastructure (other connected devices, recorders, viewers, management servers) or via physical access.

Threat landscape. The IP video devices present a usual target for remote attacks, both spontaneous and targeting specifically this type of device or the whole infrastructure supporting the surveillance of the particular area or object. For example, having emerged in 2016, the Mirai botnet remains a constant IoT security threat targeting DVRs and CCTV cameras, as well as other devices. These botnet devices can be instrumental in launching simultaneous large-scale attacks against multiple targets. Since the publication of the Mirai source code, malware authors are continuously improving their own botnets by adding new functionalities and exploits.

Relevance. IP video camera is not a principally new kind of device, and security, without any doubt, is one of its major concerns. Security best practices, regulatory and standard requirements exist for IP cameras. Specific vendor recommendations on hardening Bosch IP video surveillance camera platforms are also applicable.

Pertinence. Sometimes security incidents involving IP cameras are discussed publicly. However, such incidents occur from time to time even if they are kept out of public discussion. Bosch issues Security Advisories to inform customers about identified security vulnerabilities in their products or services.

Urgency. The security vulnerabilities of IP cameras exist and are well known. There is a certain non-zero probability of exploring new vulnerabilities in the coming time. The technologies and services provided for external access and device management require particular attention as regards security.

Threat impact. A successful attack may cause the failure of the IP camera or even affect the security of the entire infrastructure. As we consider video surveillance, privacy concerns are also in focus, e.g. unauthorized disclosure of the video of certain people who may be recognized.

Constraints. The main constraint is the necessity for the support of live and continuous recording at most places where the video surveillance is used. Any downtime leads to major disruptions. Thus, simplified configuration and reduced training are vital, and easy operation is paramount for any features of the device, including security features.

Trust. Trust is distributed across the video surveillance infrastructure. Some security aspects rely on the configuration of the video management server. Some aspects, such as recording data security, may be compromised while the data is stored. The IP cameras have a reasonable reliance on the proper protection of the rest of infrastructure and particular components. All Bosch IP video surveillance camera models under the assessment have secure cryptoprosessors that perform functions of the hardware root of trust. Different infrastructure components have different levels of trust, and trust relationships must be clearly identified to prevent the unintentional compromise of the infrastructure.

Timeline. Camera security is seen as a quality attribute by Bosch, which is why all camera projects shall perform the stage of threat and risk analysis for the products to comply with the best security practices. Bosch allocates the time and resources for security development lifecycle and implementation of security features, however, due to increased competition in the market, the resulting cost and development lead time constraints factor into the residual security risk level of the device.

Expected results. It is important to pay attention to hardening the IP cameras according to currently known incidents and common technology vulnerabilities. Threat modeling and security hardening practices are prioritized. The maturity of the security enablement domain should be aligned with the expected degree of infrastructure protection.

Dependencies. Security governance practices mostly support hardening measures, so the comprehensiveness levels for the appropriate practices probably do not exceed the levels for hardening practices.

Target Levels of Comprehensiveness and Scope of Security Practices

The following are the purposes of every security practice and appropriate level of Comprehensiveness and Scope in the Security Maturity Target for Bosch IP video surveillance camera platforms.

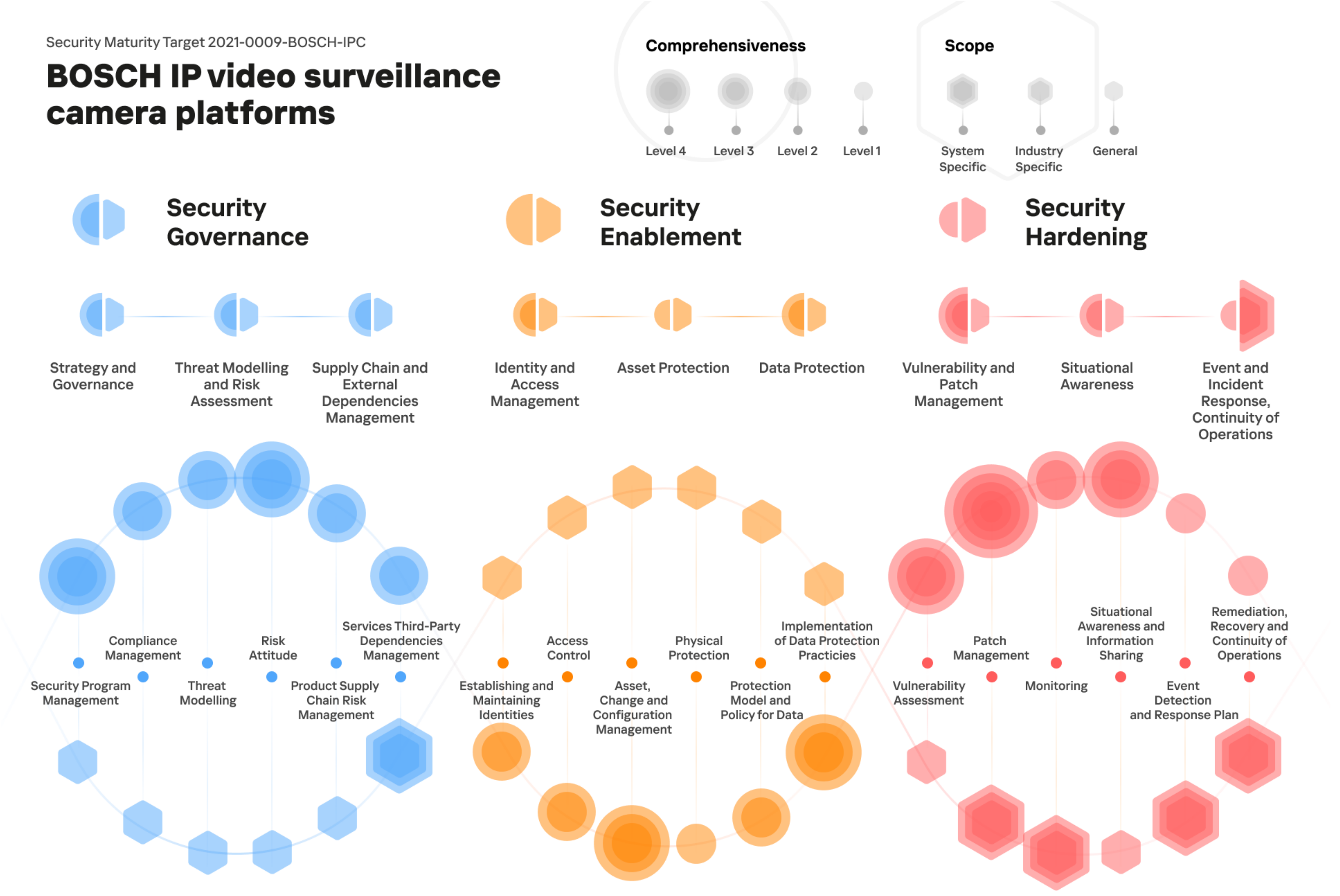
Security Practice	Purpose definition	Comprehensiveness Level	Scope Level
Security Program Management	The purpose of this practice is to cover the general topics of recognized security management standards. This means creating a security program aligned with the company's organizational structure and systems.	**3 / Consistent**	**General**
Compliance Management	The purpose of this practice is to consider some optional compliance requirements for implementation. This means applying efforts to analyze and understand compliance requirements for implementation.	**2 / Ad hoc**	**General**
Threat Modeling	The purpose of this practice is to describe and classify threats in an accurate (optionally formal) way. This means that at least performing vulnerability analysis to identify threats and addressing threats is in an ad-hoc manner according to results of risk analysis.	**2 / Ad hoc**	**General**
Risk Attitude	The purpose of this practice is to measure and appropriately manage the risks. That means establishing procedures for detailed risk assessment and differentiating the importance of risks.	**3 / Consistent**	**General**
Product Supply Chain Risk Management	The purpose of this practice is to implement some security testing for the supplied components. This means implementing analysis, contracts and methods for reviewing and protecting the supply chain.	**2 / Ad hoc**	**General**
Services Third-Party Dependencies Management	The purpose of this practice is to provide for quality of services through contractual agreements. This means providing 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.	**2 / Ad hoc**	**System**
Establishing and Maintaining Identities	The purpose of this practice is to manage the identities for several groups of people, systems or things. This means achieving dynamic device identity.	**2 / Ad hoc**	**General**

Access Control	The purpose of this practice is to consider the role of the subject and control the appropriate access rights. This also means restricting the ability of both internal and external agents to access devices and IT components.	**2 / Ad hoc**	**General**
Asset, Change and Configuration Management	The purpose of this practice is to support change management procedures for the number of assets and/or configurations. This also means managing IT and OT assets (e.g., cameras) in an integrated manner.	**3 / Consistent**	**General**
Physical Protection	The purpose of this practice is to generally constrain the access to physical assets. This means providing recommendations to restrict access to physical assets in general. The customer may want to enhance physical protection regime depending on the use case for the camera. The responsibility for the appropriate implementation of this practice is shifted to the customer.	**1 / Minimum**	**General**
Protection Model and Policy for Data	The purpose of this practice is to set simple data categorization and appropriate constraints. This means developing data classification systems in discrete environments, e.g. to understand which types of data may contain information protected by law. As the overall responsibility for protecting the data is on the customer, Bosch can't provide more specific measures to support specific policies. However, the ad hoc approach properly addresses the level of details available on the Bosch side for data protection policy definition.	**2 / Ad hoc**	**General**
Implementation of Data Protection Controls	The purpose of this practice is to support the proper application of data controls according to recognized standards. This means implementing systematic data protection measures across the entire system	**3 / Consistent**	**General**
Vulnerability Assessment	The purpose of this practice is to get an objective third-party evaluation of vulnerabilities and exposures. This means performing holistic vulnerability analysis of the IP camera as a whole using automation and third-party evaluations.	**3 / Consistent**	**General**
Patch Management	The purpose of this practice is to enforce a system policy to guarantee the continuous protection against known attacks. This means protecting components with a long lifecycle and those not easily patched due to certification or operational requirements. Bosch constrains implementation of this practice (applying the updates automatically) due to possible operational restrictions on the Customer's side. For example, video surveillance can't be stopped in an	**4 / Formalized**	**System**

	arbitrary manner for the updates. This changes the scope of the practice implementation to System.		
Monitoring	The purpose of this practice is to periodically check events indicating how properly the critical processes execute. This means obtaining status events from devices and checking for the correct expected operation. This practice implementation has several constraints. 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 with diagnostic activities. This narrows the scope of the practice to System.	**2 / Ad hoc**	**System**
Situation Awareness and Information Sharing	The purpose of this practice is to consider on a case basis sharing internal data with authorities and community. This means supporting general awareness of external incidents and implementing a policy of sharing information with external parties on a need-to-know basis.	**3 / Consistent**	**General**
Event Detection and Response Plan	The purpose of this practice is to define specific incidents and basic actions to react. This means providing guidance on how to detect and respond to incidents that can impact critical components. Only the minimum level for this practice is considered because event detection and response are the customer's responsibility. Immediate response is not always possible, as the camera may be in use. This narrows down the Scope for this practice to System and reduces the number of applicable event response methods.	**1 / Minimum**	**System**
Remediation, Recovery, and Continuity of Operations	The purpose of this practice is to give basic instructions for system recovery. This means providing basic instructions for system recovery. Remediation and recovery can only be conducted when the camera is available depending on the required surveillance regime and camera placement. This changes the Scope for this practice to System.	**1 / Minimum**	**System**

Security Maturity Target 2021-0009-BOSCH-IPC

BOSCH IP video surveillance camera platforms



Comprehensiveness

Level 4 Level 3 Level 2 Level 1

Scope

System Specific Industry Specific General

Security Governance

Strategy and Governance

Threat Modelling and Risk Assessment

Supply Chain and External Dependencies Management

Security Program Management

Compliance Management

Threat Modelling

Risk Attitude

Product Supply Chain Risk Management

Services Third-Party Dependencies Management

Security Enablement

Identity and Access Management

Asset Protection

Data Protection

Establishing and Maintaining Identities

Access Control

Asset, Change and Configuration Management

Physical Protection

Protection Model and Policy for Data

Implementation of Data Protection Practicies

Security Hardening

Vulnerability and Patch Management

Situational Awareness

Event and Incident Response, Continuity of Operations

Vulnerability Assessment

Patch Management

Monitoring

Situational Awareness and Information Sharing

Event Detection and Response Plan

Remediation, Recovery and Continuity of Operations

Figure 2 - The Security Maturity Target definition

kaspersky

www.kaspersky.com

https://ics-cert.kaspersky.com