kaspersky

Программно-аппаратные платформы IP-камер видеонаблюдения Bosch: отчет об оценке зрелости безопасности

#2021-0009-0002-EXT

Kaspersky ICS CERT

27.09.2021

kaspersky

kaspersky

О проведении оценки зрелости безопасности

Данный документ представляет собой публичный отчёт о результатах проведения оценки зрелости безопасности для IP-камер видеонаблюдения Bosch.

Оценка зрелости проводилась на основе Модели зрелости безопасности (IoT Security Maturity Model, IoT SMM), разработанной Консорциумом промышленного интернета вещей (Industry IoT Consortium). При оценке принимался во внимание *Целевой профиль зрелости безопасности*, который был разработан ранее для данной платформы и доступен по ссылке https://kas.pr/b7c6.

Отчёт подготовлен специалистами Kaspersky ICS CERT.

Объект оценки

Объектом данной оценки являются следующие IP-камеры видеонаблюдения:

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

Для анализа уязвимостей, проводимого в рамках оценки уровня зрелости безопасности, были предоставлены следующие IP-камеры:

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

Сходство функционального назначения, встроенного программного обеспечения и процессов, реализованных для обеспечения функций безопасности, позволяет распространить результаты этой оценки на следующие камеры:

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

Результаты анализа уязвимостей, проведенного как часть общей оценки, могут распространяться на камеры из данного списка не в полной мере.

Цель оценки зрелости безопасности

IP-камеры видеонаблюдения становятся все более распространены в современной сетевой среде. И, как в случае с любым IP-устройством в сети, защищённость сети от атак зависит от функционала устройства и возможностей по обеспечению его безопасности. Не существует универсального решения по обеспечению безопасности видеоданных. Разные обстоятельства требуют для камеры различного функционала обеспечения безопасности.

Тем не менее, разработчик хочет удостовериться, что существующий функционал обеспечения безопасности устройства представляет достаточно защищенную основу для отсутствия в долгосрочной перспективе существенных сомнений в безопасности видео и других типов данных, равно как и в комплексной защите сетевого окружения, где установлена данная камера.

Целью оценки уровня зрелости безопасности и повышения защищённости является поддержка эффективного, а не избыточного и произвольного, использования механизмов защиты. Для оценки одновременно применяются

показатели полноты и специфичности реализации требований безопасности[1] с одновременным учетом стоимости этой реализации. **Полнота** реализации рассматривает глубину проработки и внимание к деталям реализации требований безопасности, повышая общие гарантии защиты устройства и его окружения, а **специфичность** учитывает отраслевые требования и другие специальные условия и ограничения реализации безопасности со стороны применения системы.

Задачей оценки уровня зрелости безопасности является оценка полноты и специфичности требований безопасности для процессов разработки, использования и обслуживания устройства. Целевые уровни показателей полноты и специфичности для требований (практик) безопасности задокументированы в разработанном для устройства *Целевом профиле зрелости безопасности*.

Целевой профиль зрелости безопасности устанавливает необходимый и достаточный уровень зрелости безопасности для рассматриваемой системы. Целевой профиль состоит из перечня практик безопасности с их уровнями полноты и специфичности реализации, которые дают заинтересованным сторонам проекта понимание целей безопасности и задач каждой практики безопасности.

Метод оценки зрелости безопасности

Оценка текущего состояния зрелости безопасности проводилась посредством интервьюирования сотрудников Bosch, анализа пользовательской документации и документации по обеспечению безопасности, а также на основании результатов поиска и оценки уязвимостей IP-камер.

Интервьюирование сотрудников проводилось в два этапа:

- Первый этап заключался в заполнении опросника, вопросы которого не были сопоставлены с конкретными практиками безопасности и уровнями полноты их реализации, чтобы избежать предвзятости в ответах;
- Второй этап стартовал после обработки результатов первого этапа. На данном этапе были представлены предварительные результаты оценки полноты практик безопасности. Затем, для устранения противоречий, полученных на первом этапе, для восполнения пробелов в данных и, где необходимо, для предоставления свидетельств, подтверждающих ранее данные ответы, был использован дополнительный опросник. Также на данном этапе проводилась оценка уровня специфичности практик (общий, отраслевой или системный).

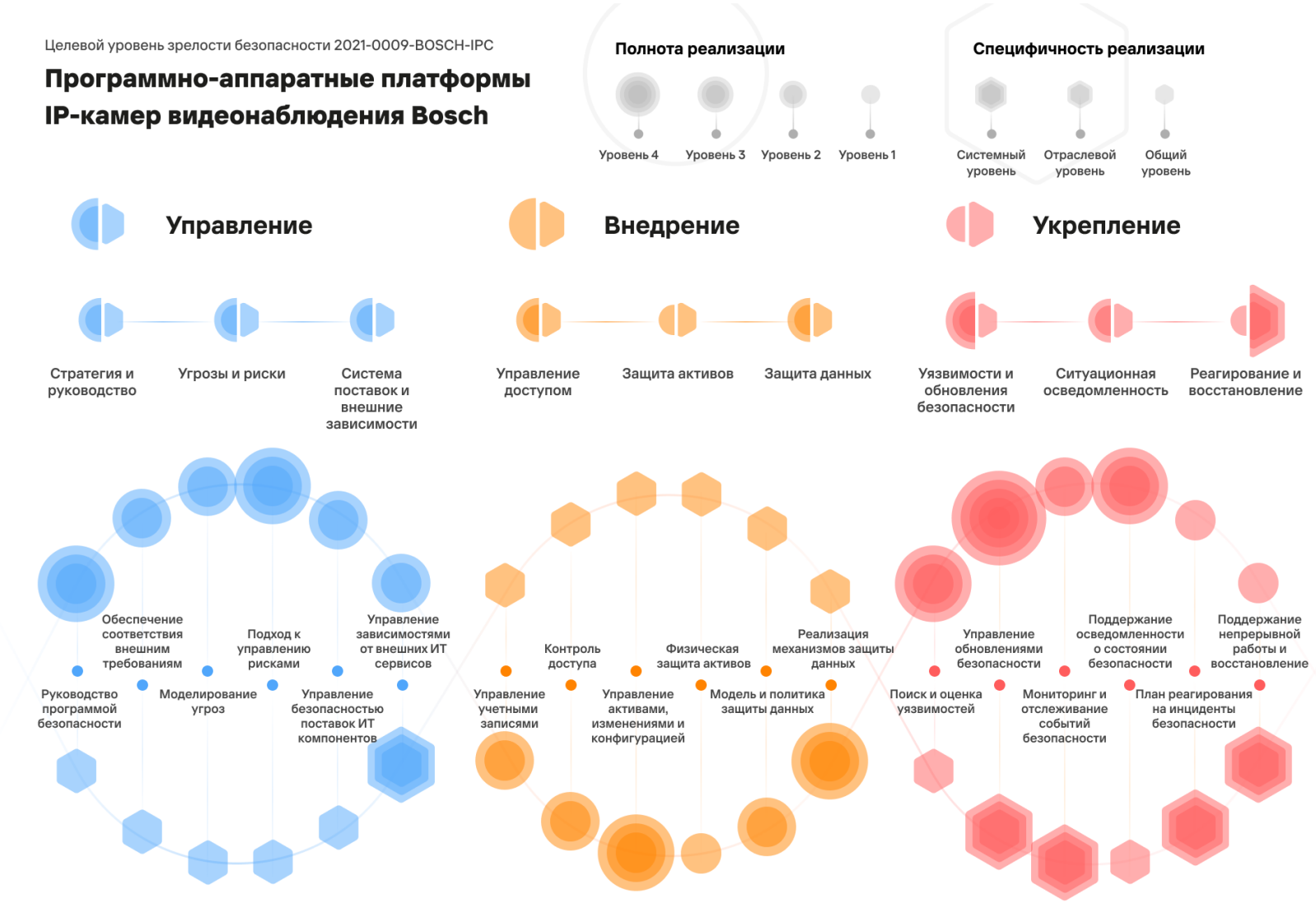
[1] Полнота реализации требований безопасности далее указывается как «полнота». Специфичность реализации требований безопасности далее указывается как «специфичность».

Оценка уязвимостей, которая проводилась как отдельная и независимая процедура, позволила получить информацию по следующим аспектам:

- Насколько заявленные уровни полноты практик соотносятся с реальной технической реализацией этих практик. Найденные и должным образом устранённые уязвимости способствовали подтверждению уровня полноты в плане технической реализации надлежащих мер безопасности;
- Насколько заявленные уровни полноты практик, в особенности связанных с поиском уязвимостей и управлением обновлениями безопасности, соответствуют действительным процессам управления уязвимостями и обновлениями. Действия, предпринимаемые командой Bosch, способствовали подтверждению, что соответствующие процессы реализованы надлежащим образом.

Результаты интервьюирования и анализа свидетельств, пользовательской документации, документации по обеспечению безопасности, а также *Отчёт о результатах поиска и оценки уязвимостей в IP-камерах* позволили сделать заключение о соответствии объектов оценки заявленному Целевому профилю зрелости безопасности.

Целевой уровень зрелости безопасности



kaspersky

Результаты оценки зрелости безопасности

Практика безопасности	Целевая полнота	Уровень полноты	Целевая специфичность	Уровень специфичности
Руководство программой безопасности	3 / Упорядоченный	3 / Упорядоченный	Общий	Общий
Обеспечение соответствия внешним требованиям	2 / Ситуативный	2+ / Ситуативный +	Общий	Общий
Моделирование угроз	2 / Ситуативный	2+ / Ситуативный +	Общий	Общий
Подход к управлению рисками	3 / Упорядоченный	3 / Упорядоченный	Общий	Общий
Управление безопасностью поставок ИТ компонентов	2 / Ситуативный	2 / Ситуативный	Общий	Общий
Управление зависимостями от внешних ИТ сервисов	2 / Ситуативный	2 / Ситуативный	Системный	Системный
Управление учётными записями	2 / Ситуативный	2 / Ситуативный	Общий	Общий
Контроль доступа	2 / Ситуативный	2 / Ситуативный	Общий	Общий

Управление активами, изменениями и конфигурацией	**3 / Упорядоченный**	**3 / Упорядоченный**	**Общий**	**Общий**
Физическая защита активов	**1 / Минимальный**	**1 / Минимальный**	**Общий**	**Общий**
Модель и политика защиты данных	**2 / Ситуативный**	**2 / Ситуативный**	**Общий**	**Общий**
Реализация механизмов защиты данных	**3 / Упорядоченный**	**3 / Упорядоченный**	**Общий**	**Общий**
Поиск и оценка уязвимостей	**3 / Упорядоченный**	**3 / Упорядоченный**	**Общий**	**Общий**
Управление обновлениями безопасности	**4 / Формализованный**	**4 / Формализованный**	**Системный**	**Системный**
Мониторинг и отслеживание событий безопасности	**2 / Ситуативный**	**2 / Ситуативный**	**Системный**	**Системный**
Поддержание осведомлённости о состоянии безопасности	**3 / Упорядоченный**	**3 / Упорядоченный**	**Общий**	**Общий**
План реагирования на инциденты безопасности	**1 / Минимальный**	**1 / Минимальный**	**Системный**	**Системный**
Поддержание непрерывной работы и восстановление	**1 / Минимальный**	**1 / Минимальный**	**Системный**	**Системный**

Руководство программой безопасности

Уровни полноты и специфичности	
	3 / Упорядоченный **Общий**
Цели обеспечения безопасности	
	Bosch стремится создать программу безопасности, исходя из своей организационной структуры и систем поддержки этой структуры.
Заключение оценки зрелости практики	
	Реализация практики представляет действия, основанные на предпочтительном плане и создании надлежащей организационной структуры. **Руководство программой безопасности соответствует уровню полноты 3 / Упорядоченный.** **Уровень специфичности – Общий.**

kaspersky

Обеспечение соответствия внешним требованиям

Уровни полноты и специфичности	
	2+ / Ситуативный + **Общий**
Цели обеспечения безопасности	
	Bosch стремится проанализировать и понять требования по соответствию, которые требуется реализовать.
Заключение оценки зрелости практики	
	Практики компании демонстрируют понимание требований по соответствию и способность проводить оценку соответствия самостоятельно либо привлекать для нее внешних исполнителей. **Обеспечение соответствия внешним требованиям соответствует уровню полноты 2+ / Ситуативный +.** **Уровень специфичности – Общий.**

kaspersky

Моделирование угроз

Уровни полноты и специфичности	
	2+ / Ситуативный + **Общий**
Цели обеспечения безопасности	
	Bosch стремится проводить анализ уязвимостей, чтобы идентифицировать угрозы. Меры по реагированию на угрозы применяются ситуативно, в зависимости от обстоятельств.
Заключение оценки зрелости практики	
	Практики компании включают оценку уязвимостей, чтобы понять, какие угрозы существуют и затрагивают ли они непосредственно рассматриваемую IP-камеру. Для моделирования угроз на основе информации об уязвимостях используются как общепризнанные методы, так и специальные средства. **Моделирование угроз соответствует уровню полноты 2+ / Ситуативный +.** **Уровень специфичности – Общий.**

kaspersky

Подход к управлению рисками

Уровни полноты и специфичности	
	3 / Упорядоченный **Общий**
Цели обеспечения безопасности	
	Bosch стремится установить процедуры по детальной оценке рисков и ранжирует риски по значимости.
Заключение оценки зрелости практики	
	У компании присутствует достаточно хорошее понимание рисков, однако управление рисками реализуется ситуативно, в зависимости от обстоятельств. **Подход к управлению рисками соответствует уровню полноты 3 / Упорядоченный.** **Уровень специфичности – Общий.**

kaspersky

Управление безопасностью поставок ИТ компонентов

Уровни полноты и специфичности	
	2 / Ситуативный **Общий**
Цели обеспечения безопасности	
	Bosch стремится реализовать процедуры анализа при заключении договоров и внедрить методы по пересмотру и защите цепочки поставок.
Заключение оценки зрелости практики	
	Для отслеживания мер безопасности, реализуемых поставщиками, и оценки эффективности данных мер, компания использует ситуативные приёмы анализа цепочки поставок товаров. **Управление безопасностью поставок ИТ компонентов соответствует уровню полноты 2 / Ситуативный.** **Уровень специфичности – Общий.**

kaspersky

Управление зависимостями от внешних ИТ сервисов

Уровни полноты и специфичности	
	2 / Ситуативный **Системный**
Цели обеспечения безопасности	
	Bosch стремится обеспечить качество сервисов посредством соглашений о качестве предоставляемых услуг и определения в соглашениях критериев исполнения обязательств. **Bosch устанавливает особые цели по отношению к определению критериев. А именно, доступность устройства должна сохраняться даже в случае отказа внешнего сервиса. Данное обстоятельство определяет уровень специфичности практики как Системный.**
Заключение оценки зрелости практики	
	Управление зависимостями от внешних ИТ сервисов отслеживает соответствие заключенным соглашениям и контролирует наличие соглашений о качестве предоставляемых услуг (SLA) и определение критериев исполнения обязательств (KPI и пр.). Нормальная работа устройства гарантируется даже в случае, если внешний сервис не доступен. **Управление зависимостями от внешних ИТ сервисов соответствует уровню полноты 2 / Ситуативный.** **Уровень специфичности – Системный.**

kaspersky

Управление учётными записями

Уровни полноты и специфичности	
	2 / Ситуативный **Общий**
Цели обеспечения безопасности	
	Bosch стремится реализовать динамическое управление идентификаторами устройств.
Заключение оценки зрелости практики	
	Камеры можно идентифицировать. Для идентификаторов с присвоенными ролями поддерживается контроль доступа к устройству. **Управление учётными записями соответствует уровню полноты 2 / Ситуативный.** **Уровень специфичности – Общий.**

kaspersky

Контроль доступа

Уровни полноты и специфичности	
	2 / Ситуативный **Общий**
Цели обеспечения безопасности	
	Bosch стремится ограничить для внутренних и внешних субъектов возможности получения доступа к устройствам и ИТ компонентам.
Заключение оценки зрелости практики	
	Контроль доступа учитывает как внешние, так и внутренние угрозы. Уязвимости в механизмах контроля доступа, найденные при проведении оценки, были устранены должным образом. Для приведения ограничения доступа в соответствие с предполагаемыми сценариями использования IP-камер, используется контроль доступа на основе ролей. **Контроль доступа соответствует уровню полноты 2 / Ситуативный.** **Уровень специфичности – Общий.**

kaspersky

Управление активами, изменениями и конфигурацией

Уровни полноты и специфичности	
	3 / Упорядоченный **Общий**
Цели обеспечения безопасности	
	Bosch стремится к комплексному управлению ИТ и ОТ активами.
Заключение оценки зрелости практики	
	Управление конфигурацией камеры реализовано комплексными и всеобъемлющими средствами. **Управление активами, изменениями и конфигурацией соответствует уровню полноты 3 / Упорядоченный.** **Уровень специфичности – Общий.**

kaspersky

Физическая защита активов

Уровни полноты и специфичности	
	1 / Минимальный **Общий**
Цели обеспечения безопасности	
	Bosch стремится ограничить доступ к физическим активам.
Заключение оценки зрелости практики	
	Что касается физической защиты активов, Bosch не предлагает множество средств защиты, поскольку камеры должны устанавливаться только обученными профессионалами с достаточными знаниями по развертыванию систем видеонаблюдения и требуемому уровню физической защиты. **Физическая защита активов уровню полноты 1 / Минимальный.** **Уровень специфичности – Общий.**

kaspersky

Модель и политика защиты данных

Уровни полноты и специфичности	
	2 / Ситуативный **Общий**
Цели обеспечения безопасности	
	Bosch стремится разработать применить требования по обеспечению безопасности разрозненных типов данных, присутствующих в предметной области.
Заключение оценки зрелости практики	
	Данные классифицируются согласно степени их влияния на бизнес и безопасность пользователей, подход к классификации данных не является системным. **Модель и политика защиты данных соответствуют уровню полноты 2 / Ситуативный.** **Уровень специфичности – Общий.**

kaspersky

Реализация механизмов защиты данных

Уровни полноты и специфичности	
	3 / Упорядоченный **Общий**
Цели обеспечения безопасности	
	Bosch стремится реализовать последовательные меры по защите данных для всей системы.
Заключение оценки зрелости практики	
	В рамках всей системы для защиты информации конфиденциального характера, хранимой на камере, а также передаваемой с камеры или на камеру, на каждом из уровней применяется несколько механизмов. Автоматизация механизмов защиты реализована при помощи хорошо зарекомендовавших себя средств. **Реализация механизмов защиты данных соответствует уровню полноты 3 / Упорядоченный.** **Уровень специфичности – Общий.**

kaspersky

Поиск и оценка уязвимостей

Уровни полноты и специфичности	
	3 / Упорядоченный **Общий**
Цели обеспечения безопасности	
	Bosch стремится проводить всеобъемлющий анализ уязвимостей для системы в целом с использованием средств автоматизации и независимых методов оценки.
Заключение оценки зрелости практики	
	Практика оценки уязвимостей Bosch удовлетворяет требованиям усиленной защиты критичных компонентов от киберпреступников, обладающих среднем уровнем навыков, и от инсайдерских атак. **Поиск и оценка уязвимостей соответствуют уровню полноты 3 / Упорядоченный.** **Уровень специфичности – Общий.**

kaspersky

Управление обновлениями безопасности

Уровни полноты и специфичности	
	4 / Формализованный **Системный**
Цели обеспечения безопасности	
	Bosch стремится защитить компоненты с продолжительным жизненным циклом и компоненты, процесс обновления которых затруднён из-за требований к эксплуатации или сертификации.
Заключение оценки зрелости практики	
	Bosch выстроил централизованный процесс управления обновлениями для своей ИТ инфраструктуры и среды разработки. Для пользовательских устройств, подключённых к порталу удаленного обслуживания (Remote Portal), предоставляются автоматизированные средства управления обновлениями. Обновления прошивки и патчи также можно скачать из репозитория Bosch (Download Store). Для совершенствования политики защиты устаревших устройств и устройств, процесс обновления которых затруднён из-за требований к непрерывности их эксплуатации, клиенты Bosch должны принимать во внимание меры и компенсационные решения, изложенные в Советах по обеспечению безопасности (Bosch Security Advisory). **Управление обновлениями безопасности соответствует уровню полноты 4 / Формализованный.** **Уровень специфичности – Системный.**

kaspersky

Мониторинг и отслеживание событий безопасности

Уровни полноты и специфичности	
	2 / Ситуативный **Системный**
Цели обеспечения безопасности	
	Bosch стремится реализовать получение сообщений об изменении состояния устройства и проверку на корректную работу устройства.
Заключение оценки зрелости практики	
	Реализация мониторинга событий безопасности включает события, поступающие от отдельных компонентов, устройств, датчиков и систем для обнаружения проблем обеспечения безопасности. Пользователи могут выстроить централизованный подход к мониторингу. Вредоносное ПО не детектируется, поскольку не признаётся в качестве актуальной угрозы. До сих пор вредоносное ПО ни разу не было обнаружено в проприетарной операционной системе, однако данное обстоятельство не означает, что оно действительно отсутствует. Чтобы обеспечить как можно более длительную работу устройства, можно применить особый подход, исключающий влияние на устройство процедур диагностики (системная эмуляция). Данный подход сужает уровень специфичности до Системного. **Мониторинг и отслеживание событий безопасности соответствуют уровню полноты 2 / Ситуативный.** **Уровень специфичности – Системный.**

kaspersky

Поддержание осведомлённости о состоянии безопасности

Уровни полноты и специфичности	
	3 / Упорядоченный **Общий**
Цели обеспечения безопасности	
	Bosch стремится поддерживать общую осведомленность о внешних инцидентах и реализовывать политику предоставления информации третьим сторонам, исходя из принципа необходимой осведомленности.
Заключение оценки зрелости практики	
	Реализация данной практики помогает Bosch получать информацию о внешних инцидентах на регулярной основе. Политика предоставления информации поддерживает ответственный подход к раскрытию информации о безопасности. **Поддержание осведомлённости о состоянии безопасности соответствует уровню полноты 3 / Упорядоченный.** **Уровень специфичности – Общий.**

kaspersky

План реагирования на инциденты безопасности

Уровни полноты и специфичности	
	1 / Минимальный **Системный**
Цели обеспечения безопасности	
	Bosch стремится предоставить разъяснения относительно процессов выявления и реагирования на инциденты, которые могут затронуть критичные компоненты.
Заключение оценки зрелости практики	
	Данная практика поддерживает предоставление информации об уязвимостях нулевого дня и применяется в случае, если проводятся мероприятия по тестированию и оценке защищённости. **План реагирования на инциденты безопасности соответствует уровню полноты 1 / Минимальный.** **Уровень специфичности – Системный.**

kaspersky

Поддержание непрерывной работы и восстановление

Уровни полноты и специфичности	
	1 / Минимальный **Системный**
Цели обеспечения безопасности	
	Bosch стремится предоставить основные инструкции по восстановлению системы.
Заключение оценки зрелости практики	
	Bosch определяет минимально необходимые шаги для устранения последствий сбоев и восстановления работоспособности камеры. **Поддержание непрерывной работы и восстановление соответствует уровню полноты 1 / Минимальный.** **Уровень специфичности – Системный.**

www.kaspersky.ru/

https://ics-cert.kaspersky.ru/