КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КАК выбирать и использовать ИБ фреймворки?

Илья Борисов
thyssenkrupp Industrial Solutions RUS

АРХИТЕКТУРА СУИБ

ОСНОВНЫЕ СТАНДАРТЫ

PCI-DSS

Стандарт безопасности данных индустрии платёжных карт

ISO 27001

Стандарт для системы управления информационной безопасностью

CIS-CSC

20 ключевых областей для повышения уровня кибербезопасности организации

NIST-CSF

Набор стандартов, руководств и лучших практик для комплексного управления ИБ

И ЕЩЁ СТАНДАРТЫ

COBIT 2019

Australian Government
Australian Signals Directorate

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

КОЛИЧЕСТВО КОНТРОЛЕЙ

PCI-DSS

Стандарт безопасности данных индустрии платёжных карт

79

ISO 27001

Стандарт для системы управления информационной безопасностью

144

CIS-CSC

20 ключевых областей для повышения уровня кибербезопасности организации

171

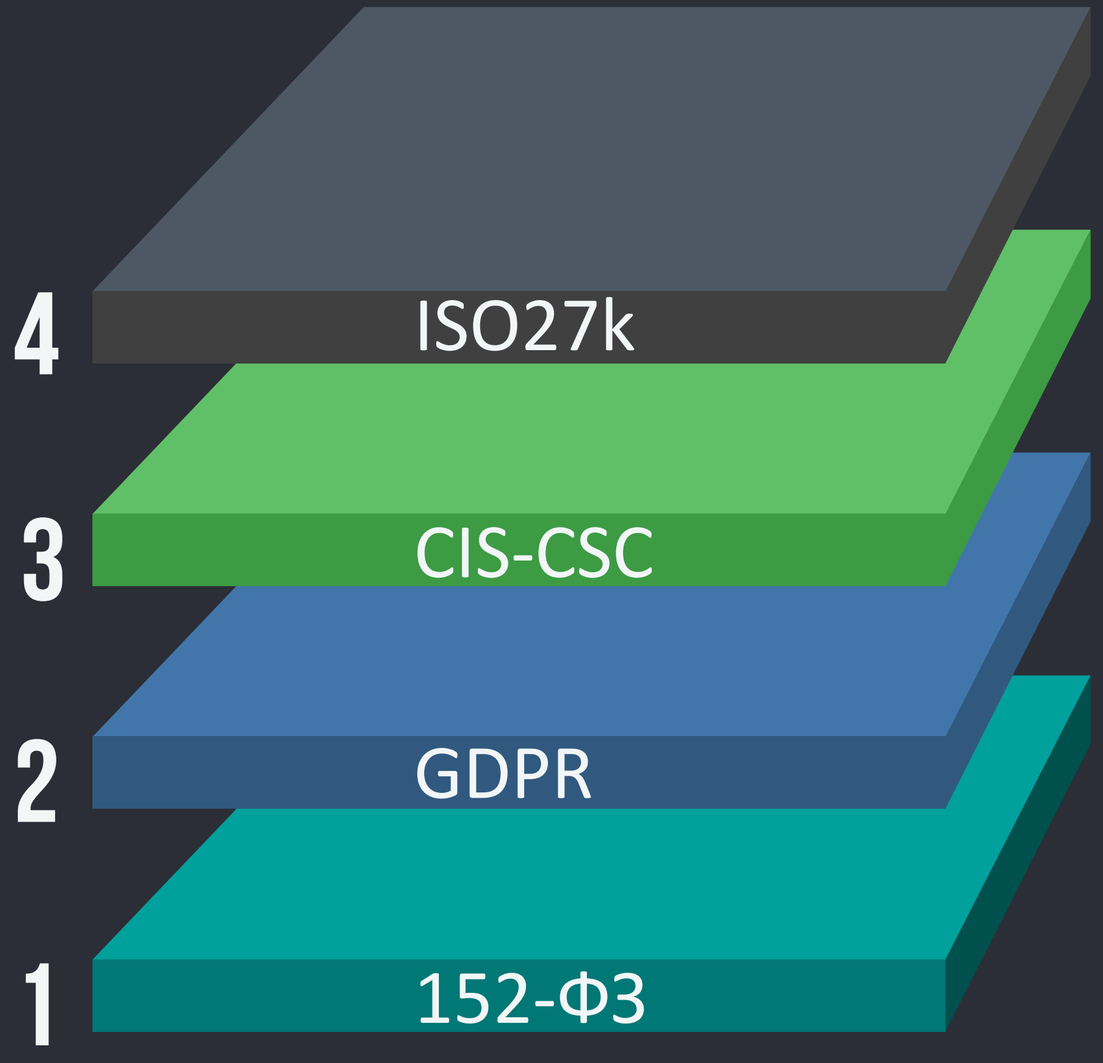
NIST-CSF

Набор стандартов, руководств и лучших практик для комплексного управления ИБ

108


1
ЦЕЛИ БИЗНЕСА
2
ТРЕБОВАНИЯ
Законодательные
Регуляторные
Международные
F
ТЕХНОЛОГИИ
Угрозы
Уязвимости
3
ПРИМЕНЕНИЕ МЕТОДОЛОГИИ
Контроли/SoA
Технические руководства
Метрики

ОПРЕДЕЛЕНИЕ ПРИОРИТЕТОВ



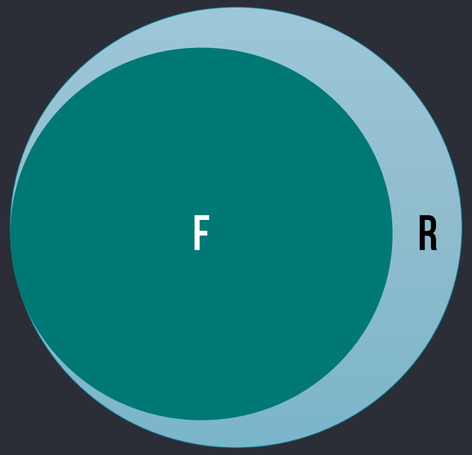
ТРЕБОВАНИЯ БИЗНЕСА

СТОИМОСТЬ ВНЕДРЕНИЯ

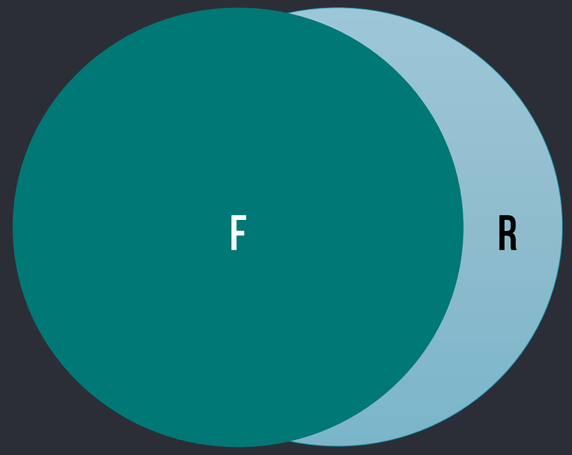
ВОЗМОЖНОСТИ ИНТЕГРАЦИИ

ВАРИАНТЫ МАППИНГА

ПОДМНОЖЕСТВО

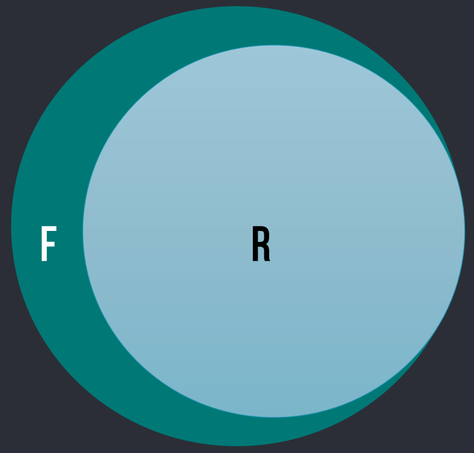


ПЕРЕСЕЧЕНИЕ

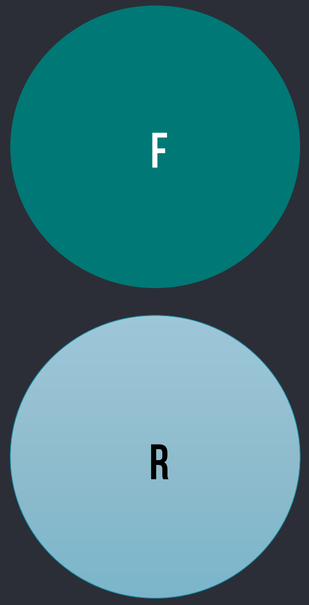


ЭКВИВАЛЕНТ

НАДМНОЖЕСТВО



НЕ СВЯЗАННЫЕ



АНТИВИРУС

CIS-CSC	ISO 27001:2013	NIST-CSF	ФСТЭК 17/21/31/239
8.1	A.12.2.1	DE.CM-4	АВ3.1
Malware Defenses	**Controls against malware**	**Malicious code is detected**	**Антивирусная защита (АВ3)**
Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures	Реализация антивирусной защиты

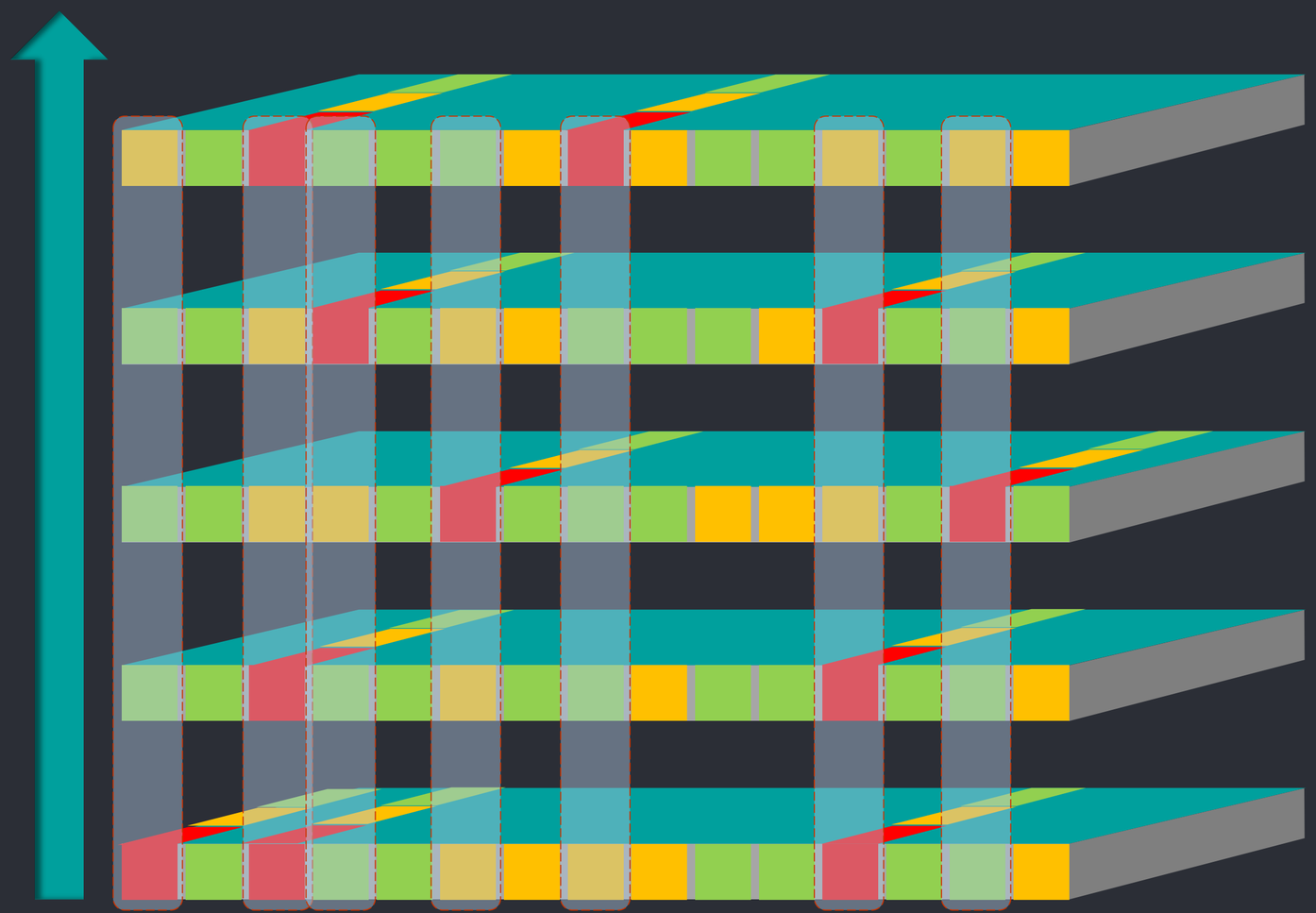
СООТВЕТСТВИЕ VS ЭФФЕКТИВНОСТЬ

VS

МОДЕЛЬ ЗРЕЛОСТИ АВЗ

	$ УРОВЕНЬ 1	$$ УРОВЕНЬ 2	$$$$ УРОВЕНЬ 3	$$$$$$ УРОВЕНЬ 4
ИНТЕГРАЦИЯ	НЕТ	СБОР ЛОГОВ, УВЕДОМЛЕНИЯ, SIEM	КОРРЕЛЯЦИЯ С ДАННЫМИ ИЗ ДРУГИХ СИСТЕМ, SIEM	ИНТЕГРАЦИЯ ЧЕРЕЗ API
ОБНАРУЖЕНИЕ	СИГНАТУРЫ	1 ИСТОЧНИК TI ПРОСТЫЕ IOC	РЕПУТАЦИЯ ЭВРИСТИКА	НЕСКОЛЬКО TI АНАЛИЗ ПОВЕДЕНИЯ
АВЗ.1	РЕАЛИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ			

СИНЕРГИЯ



БИЗНЕС-ТРЕБОВАНИЯ

ISO 27K

GDPR

КТ

КИИ

ВЫВОДЫ

СТРУКТУРА ИДЕНТИЧНА

РАЗНЫЙ ОХВАТ

РИСК-МЕНЕДЖМЕНТ

МАППИНГ

ПРОФИЛИ ПРИОРИТЕТЫ МЕТРИКИ

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

ilya.borisov@thyssenkrupp.ru
facebook.com/ilya.borisov.104