КОД ИБ

САНКТ-ПЕТЕРБУРГ

ЦИФРОВИЗАЦИЯ "БУМАЖНОЙ" ИБ

НИКОЛАЙ КАЗАНЦЕВ

CEO

SECURITM.ru

18 апреля 2024

Санкт-Петербург

Коротко обо мне

Образование

Специалитет и аспирантура на кафедрекомплексного обеспечения информационной безопасности
ГУМ РФ им. Адм. Макарова

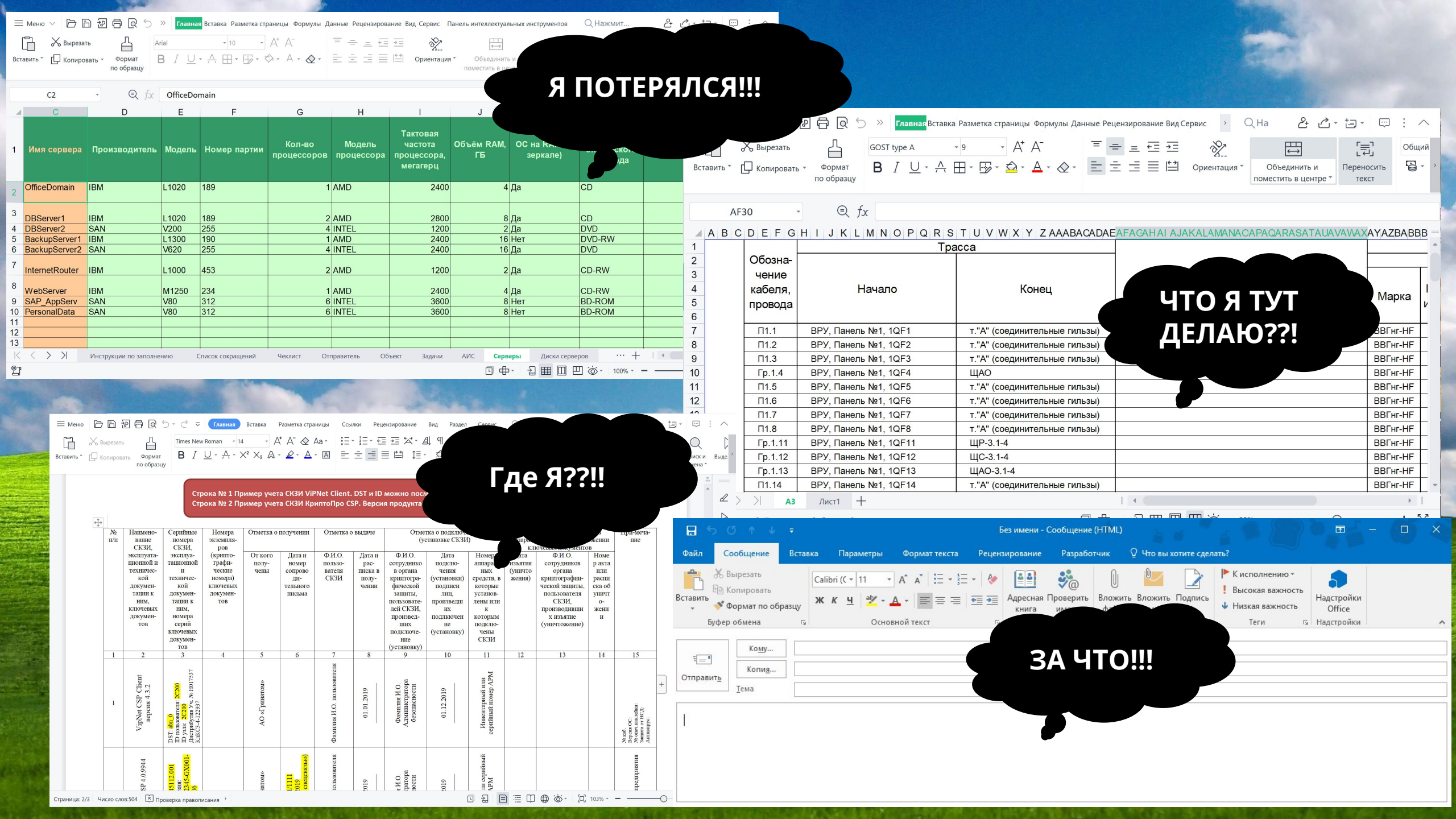
Опыт работы

CEO SECURITM.ru
В ИБ с 2010, работал в Лаборатории противодействия промышленному шпионажу, Администрации Санкт-Петербурга, начальником отдела ИБ в фарм-компании ПОЛИСАН

Сертификаты

ECCouncil CEH, Comptia Security+,
Медаль ФСТЭК за заслуги в области защиты информации

Основатель securitm.ru
Блог spbsecurity.blogspot.com



Имя сервера	Производитель	Модель	Номер партии	Кол-во процессоров	Модель процессора	Тактовая частота процессора, мегагерц	Объём RAM, ГБ	ОС на RAID-зеркале)	
OfficeDomain	IBM	L1020	189	1	AMD	2400	4	Да	CD
DBServer1	IBM	L1020	189	2	AMD	2800	8	Да	CD
DBServer2	SAN	V200	255	4	INTEL	1200	2	Да	DVD
BackupServer1	IBM	L1300	190	1	AMD	2400	16	Нет	DVD-RW
BackupServer2	SAN	V620	255	4	INTEL	2400	16	Да	DVD
InternetRouter	IBM	L1000	453	2	AMD	1200	2	Да	CD-RW
WebServer	IBM	M1250	234	1	AMD	2400	4	Да	CD-RW
SAP_AppServ	SAN	V80	312	6	INTEL	3600	8	Нет	BD-ROM
PersonalData	SAN	V80	312	6	INTEL	3600	8	Нет	BD-ROM

Обозначение кабеля, провода	Трасса: Начало	Трасса: Конец	Марка
П1.1	ВРУ, Панель №1, 1QF1	т."А" (соединительные гильзы)	ВВГнг-HF
П1.2	ВРУ, Панель №1, 1QF2	т."А" (соединительные гильзы)	ВВГнг-HF
П1.3	ВРУ, Панель №1, 1QF3	т."А" (соединительные гильзы)	ВВГнг-HF
Гр.1.4	ВРУ, Панель №1, 1QF4	ЩАО	ВВГнг-HF
П1.5	ВРУ, Панель №1, 1QF5	т."А" (соединительные гильзы)	ВВГнг-HF
П1.6	ВРУ, Панель №1, 1QF6	т."А" (соединительные гильзы)	ВВГнг-HF
П1.7	ВРУ, Панель №1, 1QF7	т."А" (соединительные гильзы)	ВВГнг-HF
П1.8	ВРУ, Панель №1, 1QF8	т."А" (соединительные гильзы)	ВВГнг-HF
Гр.1.11	ВРУ, Панель №1, 1QF11	ЩР-3.1-4	ВВГнг-HF
Гр.1.12	ВРУ, Панель №1, 1QF12	ЩС-3.1-4	ВВГнг-HF
Гр.1.13	ВРУ, Панель №1, 1QF13	ЩАО-3.1-4	ВВГнг-HF
П1.14	ВРУ, Панель №1, 1QF14	т."А" (соединительные гильзы)	ВВГнг-HF

Строка № 1 Пример учета СКЗИ ViPNet Client. DST и ID можно посм
Строка № 2 Пример учета СКЗИ КриптоПро CSP. Версия продукта

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении: От кого получены	Отметка о получении: Дата и номер сопроводительного письма	Отметка о выдаче: Ф.И.О. пользователя СКЗИ	Отметка о выдаче: Дата и расписка в получении	Отметка о подключении (установке СКЗИ): Ф.И.О. сотрудника органа криптографической защиты, пользователей СКЗИ, производивших подключение (установку)	Дата подключения (установки) подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	Примечание
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	ViPNet CSP Client версия 4.3.2	DST: abn_0 ID пользователя: 2C200 ID узла: 2C200 Дистрибутив: № Н017537 КМКЗ-4-122937		АО «Гринатом»		Фамилия И.О. пользователя	01.01.2019	Фамилия И.О. Администратора безопасности	01.12.2019	Инвентарный или серийный номер АРМ				№ каб. Версия ОС: Версия ПО ViPNet: Защита от НСД: Антивирус:
	SP 4.0.9944	5112/001 зии: 2345-GX001- 6		атом»	1111 2019 специально)	пользователя	2019	а И.О. ратора ности	2019	ли серийный АРМ				предприятия

Страница: 2/3 Число слов:504 Проверка правописания

Без имени - Сообщение (HTML)

Файл Сообщение Вставка Параметры Формат текста Рецензирование Разработчик Что вы хотите сделать?

Вставить Вырезать Копировать Формат по образцу — Буфер обмена

Calibri (С 11 — Основной текст

Адресная книга Проверить имена Вложить файл Вложить элемент Подпись

К исполнению Высокая важность Низкая важность — Теги

Надстройки Office — Надстройки

Отправить

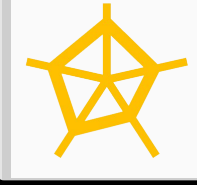
Кому...

Копия...

Тема

Чем больше инвестиций в безопасность – тем меньше эффективность

Развитие системы защиты



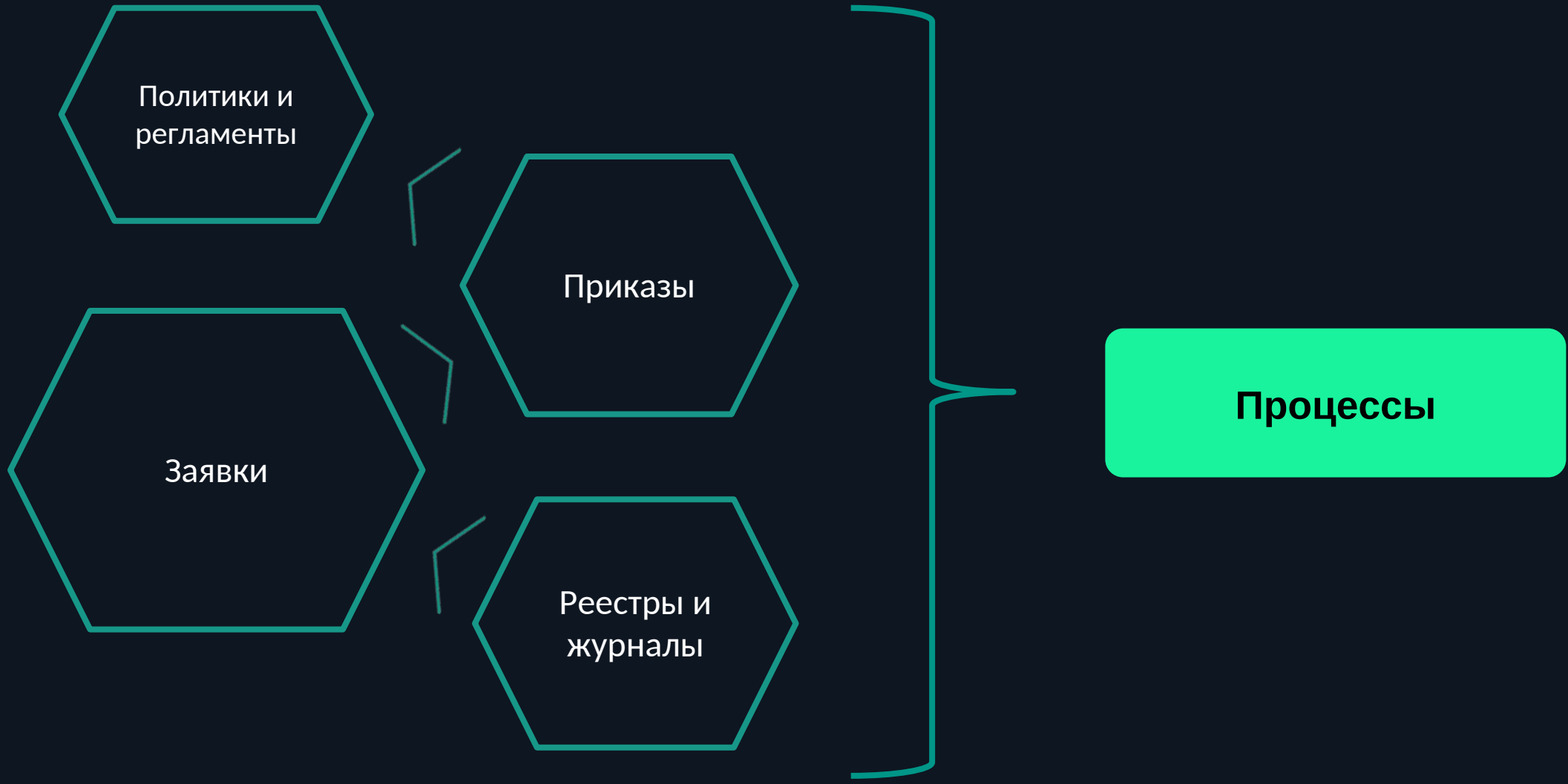
Рост количества процессов, рутины и ошибок

Деградация системы защиты

> **40%** утечек и нарушений происходят из-за **низкой эффективности процессов** в службе безопасности*

* Исследования vc.ru и tadviser.ru

Что такое «бумажная» ИБ ?



ИБ: Процессы: Документы

SECURITM решает проблему деградации систем защиты

ИТ Инфраструктура

- ✅ API
- ✅ PowerShell/Python
- ✅ Active Directory
- ✅ Qualys, Nessus, RedCheck, Nmap, OpenVas, XSpider, MaxPatrol 8/VM, ZAP, AppScreener, Snyk
- ✅ Samba
- ✅ Kaspersky
- ✅ Zabbix
- ✅ Jira
- ✅ NetBox
- ✅ Scan Factory
- ✅ Cloud Adviser
- ✅ Excel/CSV
- ✅ Mail
- ✅ Telegram
- ✅ ...

Процессы управления

- Управление рисками
- Соответствие требованиям
- Управление мерами
- Управление метриками

SECURITM

SGRC система для управления организационными процессами в информационной безопасности

Операционные процессы

- Управление активами #ITAM
- Управление уязвимостями #VM
- Автоматизация процессов #RPA
- Задачи
- Опросы
- Заявки

Сервис управления ин

service.securitm.ru

Сервис управления информационной безопасностью SECURITM

SECURITM

85 %

49

Николай
Для примера

ГЛАВНАЯ
МОИ ДЕЛА
АКТИВЫ
РИСКИ
ТРЕБОВАНИЯ
ЗАЩИТНЫЕ МЕРЫ
ТЕХНИЧЕСКИЕ УЯЗВИМОСТИ
ЗАДАЧИ
ОПРОСЫ
RPA
ОБЛАСТИ

156
Неприемлемых рисков

Текущий риск

Уровень соответствия

Защитные меры
Идет 12 внедрений
7 нарушений срока
14 мер сломано

26
Активных задач

П
З
Б
Задачи

Требования
40 / 4115

Угрозы
60

Меры
88

Каталоги
MITRE
БДУ ФСТЭК

Риски
193

Задачи
26 +3

Уязвимости
134

RPA
5

Технические уязвимости
438

Активы
205 активов
114 типов

Опросы
40 +2

Наш подход

- ✓ **Универсальные подходы** под любую отрасль
  ПДн / КИИ / ГИС / ISO / CIS / 57580 / ...
- ✓ **Бесплатная Community база знаний**
  с проектами рисков и защитных мер
- ✓ **Бесплатный доступ**
  по Community подписке
- ✓ **Социальная платформа**
  для обмена опытом между службами безопасности
- ✓ **Платформа обучения** для ВУЗов
- ✓ **Открытый прайс**

Что дальше?

Продолжить делать «бумажные» процессы ИБ

Делать автоматизированные процессы

t.me/SECURITM

Николай Казанцев
nk@securitm.ru
securitm.ru