КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Штабные киберучения

16.03.2022

Николай Казанцев
CEO **securitm.ru**

Коротко обо мне

- **Образование**
  Специалитет и аспирантура на кафедре комплексного обеспечения информационной безопасности ГУМ РФ им. Адм. Макарова.

- **Опыт работы**
  В ИБ с 2010, работал в службах ИБ государственных и коммерческих компаний. Последнее место нач.отдела ИБ «НТФФ «ПОЛИСАН»

  Создатель GRC системы SECURITM

- **Сертификаты**
  EC Council CEH, Comptia Security+, Медаль ФСТЭК за укрепление государственной системы защиты информации

- Блог spbsecurity.blogspot.com

SECURITM решает проблему деградации систем защиты

SECURITM – это система класса **sGRC** (Security Government, Risk and Compliance), которая помогает службам информационной безопасности средних/крупных компаний автоматизировать свои процессы управления безопасностью на единой платформе.

ФУНКЦИОНАЛ

- ✓ Управление **рисками** безопасности
- ✓ Контроль **соответствия** требованиям (Compliance)
- ✓ Управление **активами** (ITAM)
- ✓ Планирование, **задачи** и процессы
- ✓ Управление **уязвимостями** (VM)
- ✓ Проведение **опросов**
- ✓ **RPA**

Для продаж – CRM,
для ИТ – Jira,
для безопасности – SECURITM

Зачем проводить штабные киберучения?

Зачем проводить штабные киберучения?

- ✓ Проверка работоспособности планов реагирования на инциденты;
- ✓ Совершенствование навыков ответственных лиц;
- ✓ Выявление темных пятен в подготовке специалистов и инфраструктуре;
- ✓ Формирование понимания последствий от инцидентов;
- ✓ Сплочение команды реагирования;
- ✓ Исполнение требований регуляторики и стандартов.

Нормативные требования

- Приказ ФСТЭК России № 31 от 14.03.2014 9зжлния":
  ДНС.2 Обучение и отработка действий персонала в нештатных ситуациях

- ГОСТ Р № ИСО/МЭК 27001-2021 от 01.01.2022 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования - Приложение А":
  A.16.1.1 Обязанности и процедуры Мера обеспечения информационной безопасности: Должны быть установлены обязанности и процедуры менеджмента для обеспечения уверенности в быстром, эффективном и надлежащем реагировании на инциденты информационной безопасности

- Приказ ФСТЭК России № 239 от 25.12.2017 "Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости":
  ДНС.2 Обучение и отработка действий персонала в нештатных ситуациях

- CIS Critical Security Controls v8 (The 18 CIS CSC):
  17.4 Establish and Maintain an Incident Response Process

- NIST Cybersecurity Framework:
  RS.CO-1: Персонал знает свои роли и порядок действий, при выполнении мероприятий по реагированию

- CIS Critical Security Controls v7.1 (SANS Top 20):
  CSC 19.1 Document Incident Response Procedures

- SWIFT Customer Security Controls Framework v2022:
  7.1 Cyber Incident Response Planning