Дмитрий Кузнецов
Директор по методологии и стандартизации
dkuznetsov@ptsecurity.com

Технические средства противодействия компьютерным атакам

Драйверы защиты от компьютерных атак

POSITIVE TECHNOLOGIES

	Надзор	Риски	Ответственность	Практика
Органы власти	Да	Нет	Отчасти	Нет
Гос. корпорации	Отчасти	Нет	Да	Отчасти
Субъекты КИИ	Нет	Нет	Да	Отчасти
Крупный бизнес	Нет	Нет	Нет	Да
Малый и средний бизнес	Нет	Нет	Нет	Нет

Особенности регулирования

POSITIVE TECHNOLOGIES

- “*Применяемые системы обнаружения вторжений должны включать компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил*” (методический документ ФСТЭК)

Выбор реализации оставлен проектировщику системы защиты

- “*ФБО должны выполнять анализ собранных данных с целью обнаружения вторжений с использованием сигнатурных методов, эвристических методов и [назначение: другие методы].*” (профиль защиты)

Руководствуемся здравым смыслом

POSITIVE TECHNOLOGIES

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

CIS Controls

NIST Cybersecurity Framework

Средства предупреждения атак это…

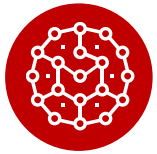
POSITIVE TECHNOLOGIES

Основные

Встроенные функции безопасности приложений

Управление конфигурацией

Антиспам



САЗ

FW, NGFW, AF

Вспомогательные

Антивирус

IPS

СЗИ НСД

СКЗИ

Фильтрация DDoS

Факторы неэффективности

POSITIVE TECHNOLOGIES

Переоценка эффективности

“Изолированные сети”

“У нас все аттестовано”

“Уникальный софт, уникальные протоколы”

Непонимание технологии

Организационные трудности

“Только одобренное”

“Только сертифицированное”

“Вендор дает нам такую скидку!”

Трудности кооперации

“Задача ИБ – контролировать ИТшников”

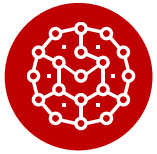
Средства обнружения атак это…

POSITIVE TECHNOLOGIES

Основные

Встроенные функции безопасности приложений

Уведомления



SIEM

Антивирусы

FW, NGFW, AF

Вспомогательные

Honeypot

IDS/IPS

“Песочницы”

Обнаружение атак – это анализ событий

POSITIVE TECHNOLOGIES

- Операционные системы, СУБД
- Приложения
- Сетевое оборудование
- Active Directory, SSO
- Сетевые службы
- Веб-серверы, WAF, IDS
- IDS, NGFW, антивирусы
- Наложенные средства защиты
- Пассивный анализ трафика

Анализ событий – это SIEM

POSITIVE TECHNOLOGIES

- Нормализация (приведение к единому формату)
- Агрегирование (объединение однотипных событий)
- Корреляция
  - Сопоставление по причинно-следственным связям
  - Сопоставление с разными источниками
- Обогащение
  - Сопоставление с уязвимостями
  - Сопоставление с инвентарными данными
  - Сопоставление с индикаторами компрометации
  - Фильтрация “ложных срабатываний”
- Ретроспективный анализ
  - Поиск устройств, уязвимых к атаке
  - Поиск новых индикаторов компрометации в архивных данных
  - Применение новых правил корреляции к архивным данным

События невозможно анализировать “вручную”!!!

Факторы неэффективности

POSITIVE TECHNOLOGIES

- Переоценка собственной компетентности
- Переоценка краудсорсинга
- Переоценка технических возможностей
- Погоня за модой
- Неготовность к успешному обнаружению

— Вот мы и здесь. Ну и что?

Реагирование на атаки – это процесс

POSITIVE TECHNOLOGIES

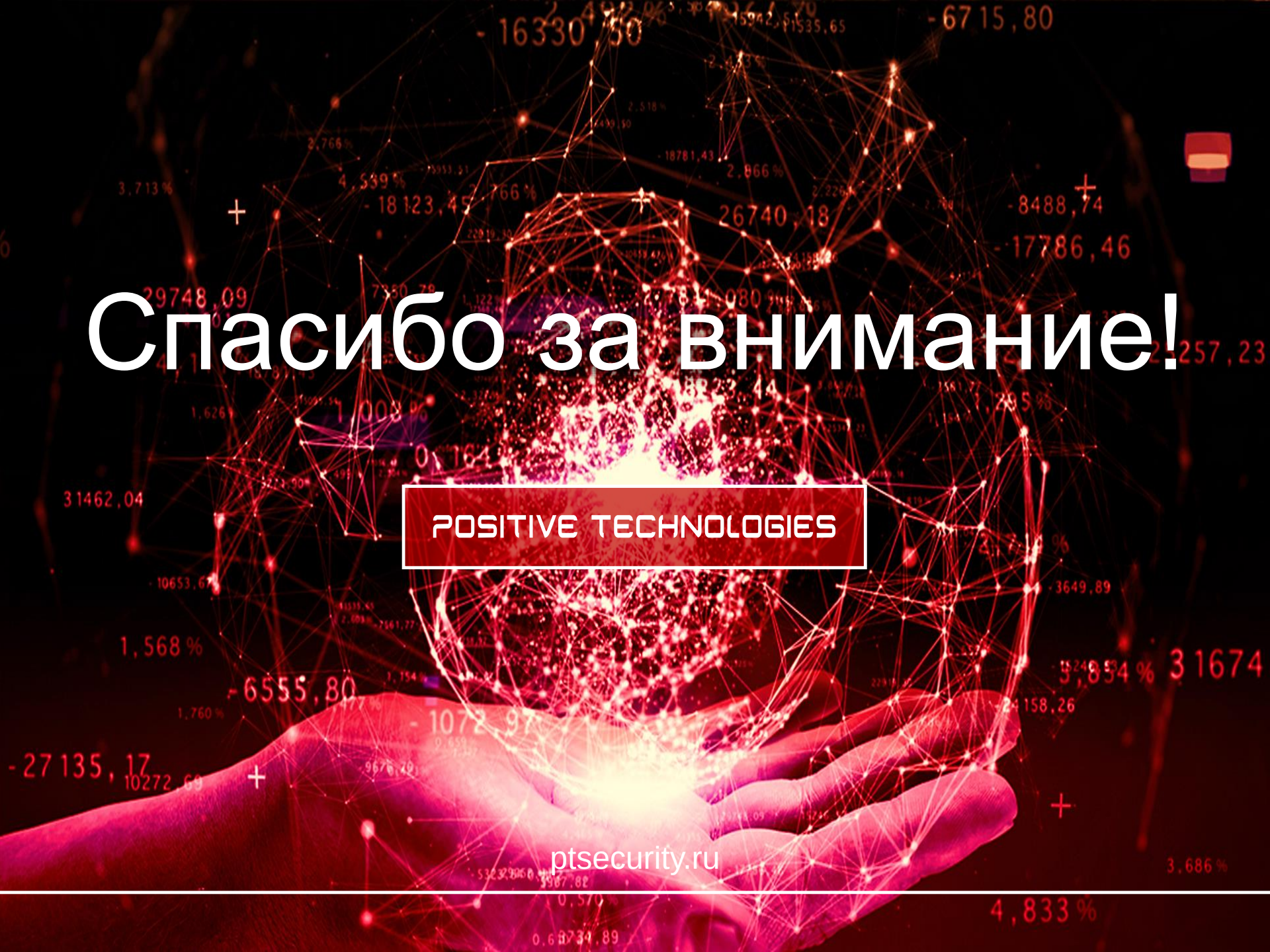
Ведение карточек инцидентов

Сбор и сохранение свидетельств

Регистрация и контроль исполнения принятых решений

Интеграция с системами управления заявками

Контроль SLA


Спасибо за внимание!
POSITIVE TECHNOLOGIES
ptsecurity.ru