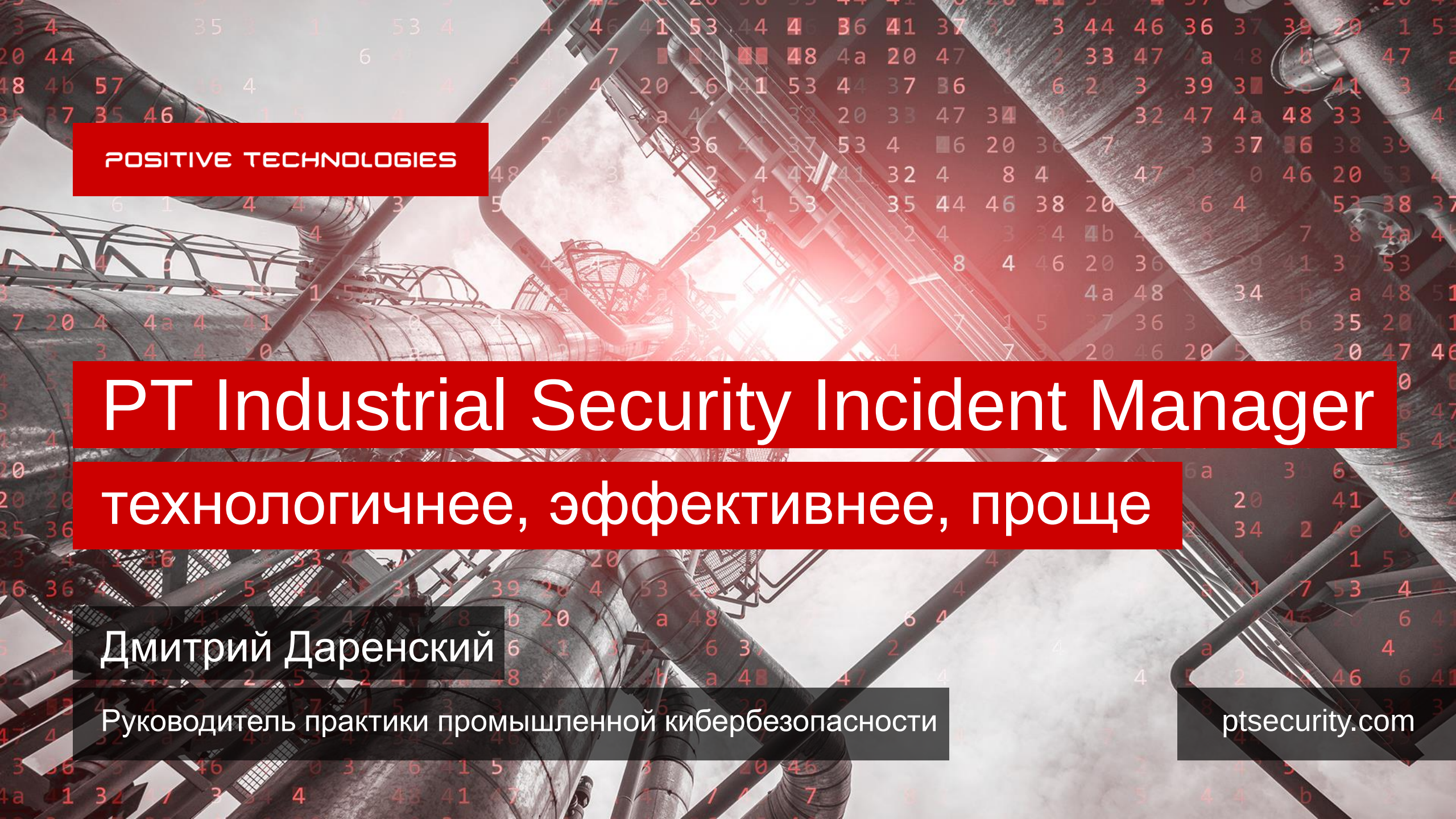


POSITIVE TECHNOLOGIES

PT Industrial Security Incident Manager

технологичнее, эффективнее, проще

Дмитрий Даренский

Руководитель практики промышленной кибербезопасности

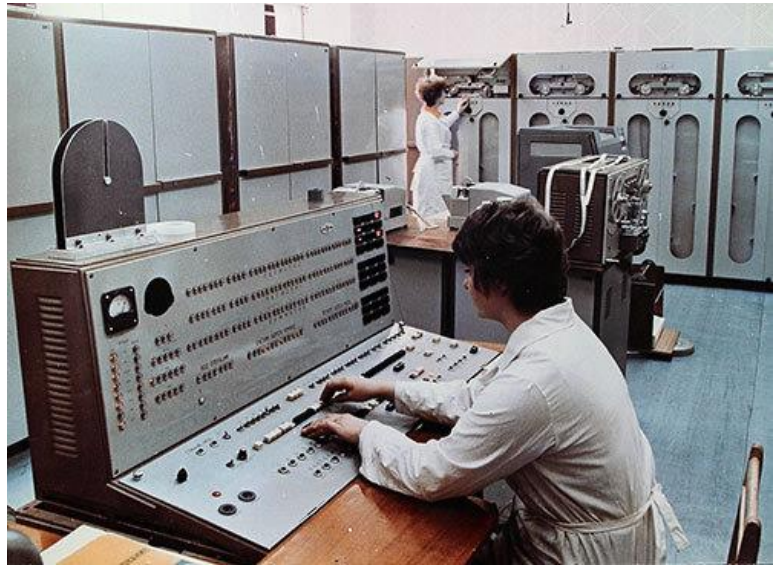
ptsecurity.com

АСУ ТП и кибербезопасность

POSITIVE TECHNOLOGIES

- История АСУ ТП — более 50-ти лет
- История ИБ АСУ ТП — менее 10-ти лет

Основной упор при разработке и эксплуатации систем АСУ ТП - на функциональную безопасность и надежность



НО! Повсеместное применение вычислительных сетей на базе Ethernet/IP и необходимость в интеграции с корпоративными системами добавили абсолютно новые риски и уязвимости

АСУ ТП основа эффективного производства и конкурентоспособности

POSITIVE TECHNOLOGIES

но какой уровень доверия к самим АСУ ТП?

Positive Technologies ежегодно находит десятки критичных уязвимостей в компонентах АСУ ТП

MOXA · SIEMENS · Honeywell · EMERSON · Schneider Electric · YOKOGAWA · CISCO · HIRSCHMANN A BELDEN BRAND

MOXA · SIEMENS · Schneider Electric · GE Energy · CISCO · HIRSCHMANN A BELDEN BRAND · ABB · PHOENIX CONTACT

BOMBARDIER · SIEMENS · Schneider Electric · ALSTOM · CISCO · HIRSCHMANN A BELDEN BRAND

MOXA · SIEMENS · Schneider Electric · Rockwell Automation · CISCO · HIRSCHMANN A BELDEN BRAND

Если в АСУ ТП нет проблем

POSITIVE TECHNOLOGIES

то почему все крупные государства озаботились безопасностью своей критической инфраструктурой?

Department for Business, Energy & Industrial Strategy

CIVIL NUCLEAR CYBER SECURITY STRATEGY

Подписан закон о безопасности критической информационной инфраструктуры

Владимир Путин подписал Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации».

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 6 July 2016

concerning measures for a high common level of security of network and information systems across the Union

Recommended Practice: Improving Industrial Control System Cybersec with Defense-in-Depth Strategies

Industrial Control Systems Cyber Emergency Response T

September 2016

Homeland Security

President Signs Critical Cyber Security Bills into Law

Friday, December 19, 2014

WASHINGTON – President Obama signed into law Thursday four bipartisan bills that will modernize, strengthen, and improve our nation's cyber security defenses. The measures are the first major cyber security bills to become law in several years.

Крайне низкая защищенность от проникновения в корпоративную сеть

73%

- 73% промышленных компаний демонстрируют недостаточную защиту периметра

- Большинство недостатков безопасности на сетевом периметре связаны с ошибками конфигурации

82%

- 82% промышленных компаний не защищены от проникновения в технологическую сеть

Администраторы сами создают небезопасные каналы управления

100%

- Недостатки сегментации и фильтрации обнаружены в 100% обследованных промышленных компаний.

64%

- В 64% компаний недочеты фильтрации и ошибки конфигурации были внесены администраторами при создании удаленных каналов управления.

18%

- В 18% компаний технологические сети не отделены от корпоративных сегментов вовсе

Большинство атак не требуют экспертных навыков от нарушителя

Более 60% векторов атак с целью проникновения в технологический сегмент характеризуются низким уровнем сложности..

- Ошибки в конфигурациях сетевых устройств
- Недостатки сегментации и межсетевой фильтрации
- Доступные в публичном пространстве эксплойты

Вместо абстрактных цифр

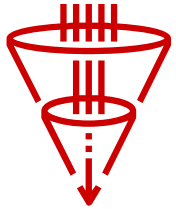
POSITIVE TECHNOLOGIES

Горно- обогатительный комбинат, пилот PT ISIM	Через сетевой сегмент АСУ ТП на 10 сетевых узлов ходит трафик всего производственного участка, включая трафик сети заводоуправления
Инструментальный анализ сети металлургического комбината	В сети АСУ ТП оказался принтер с WI-FI. Показана атака на контроллер производственной линии через функцию копирования документов
Большая электростанция, эксплуатация внедренного PT ISIM	В сети выявлено несколько сотен сетевых узлов. Эксплуатация смогла опознать как «свои» меньше половины устройств. По остальным нет информации.
Стенд компании разработчика АСУ ТП, тестирование PT ISIM	Стенд АСУ ТП оказался подключен к внутренней сети компании. В сети выявлен трафик майнеров криптовалюты, уязвимых сервисов и протоколов

Продолжать можно долго

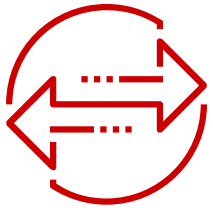
Проблемы кибербезопасности промышленных инфраструктур

POSITIVE TECHNOLOGIES



- **Взаимопроникновение ИТ и АСУ ТП**

  - Недостатки сегментации и фильтрации
  - Непрозрачное управление сетевыми активами АСУ ТП
  - Уязвимости компонентов сетей АСУ ТП

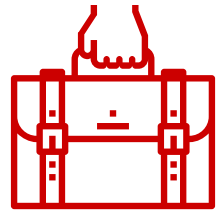


- **Недостаток контроля сетевого взаимодействия**

  - Недокументированные возможности систем АСУ ТП
  - Неуправляемый удаленный доступ к АСУ ТП
  - Наличие нелегитимных подключений и постороннего трафика

- **Отсутствие контроля конфигураций**

  - Отсутствие контроля версионности PLC и SCADA проектов
  - Бесконтрольное изменение конфигураций
  - Невозможность проведения расследований в случае инцидентов и аварий

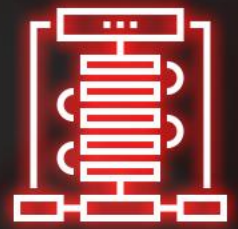


- **Вредительство и мошенничество**

  - Неавторизованное изменение параметров работы систем
  - Причинение ущерба оборудованию и репутации предприятия

PT ISIM для предприятия

Автоматическое
обнаружение кибератак



Автоматический контроль
информационного
взаимодействия в АСУ ТП

Автоматическая
инвентаризация
сетевых активов АСУ ТП

Выявление
неавторизованного
управления системами

Обеспечение соответствия
требованиям регуляторов

Поддержка процессов
реагирования и асследования
инцидентов ИБ

Референсы

POSITIVE TECHNOLOGIES

Применяется

Россия

Внедряется

Россия, Италия

Тестируется

Россия, Казахстан, Беларусь, Корея

PT ISIM

POSITIVE TECHNOLOGIES

- Непрерывный мониторинг защищенности
- Автоматическая инвентаризация сети АСУ ТП
- Анализ и корреляция событий сетевого и прикладного уровня
- Эффективное управление инцидентами ИБ
- Поддержка основных платформ АСУ ТП
- Нулевое влияние на технологическую сеть
- Оперативное информирование на всех уровнях управления
- Распределенная архитектура, интеграция с SOC
- Соответствие требованиям регуляторов (ГосСОПКА, ФСТЭК)

Объединяет стандартные и уникальные технологии Positive Technologies в одном решении

Стандартные:

- DPI / Traffic analysis, event normalization
- IDS / Network attack detection
- SIEM / Event correlation
- Inventory / Assets management
- Incident management
- Hosts, communication & events white listening

Уникальные:

- **PT ISTI** / Expert industrial threat base
- Parsing SCADA projects
- Customizing incidents network & application level
- Model correlation technology
- Attack chain detecting and visualization
- Technological process, network topology and incidents real time visualization

Компоненты PT ISIM

PT ISIM View Sensor

Анализатор трафика промышленной сети

PT ISIM Overview Center

Централизованное управление

PT ISIM View Sensor – мощный анализатор сетевого трафика

PT ISIM View Sensor

Анализатор сетевого трафика АСУ ТП (сенсор)

Поставляется в виде ПАК

Сенсор PT ISIM позволяет:

- Проводить автоматическую инвентаризацию элементов сети АСУ ТП
- Выявлять недостатки ИБ и детектировать атаки на компоненты АСУ ТП, используя встроенную базу данных угроз **PT ISTI***
- Выявлять нелегитимное управление оборудованием

✓ пуск/останов ПЛК

✓ загрузка/выгрузка проектов ПЛК

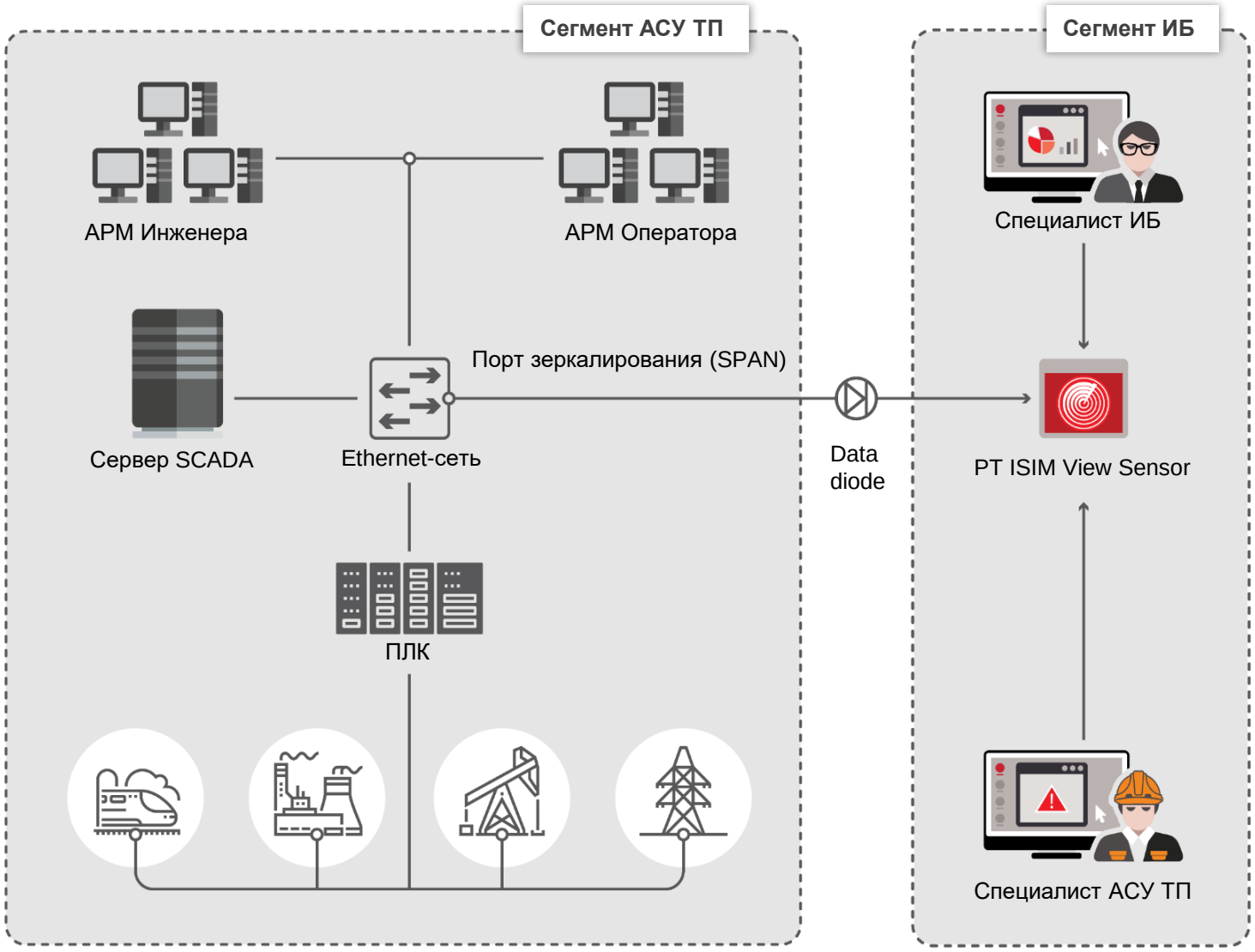
✓ обновление прошивки ПЛК

✓ использование недокументированных функций ПЛК

✓ неавторизованное изменение уставок

- Выявлять аномалии на сетевом и прикладном уровне

PT ISIM View Sensor – схема развертывания



- Архитектура пассивного мониторинга PT ISIM исключает нежелательное воздействие на техпроцесс
- Процесс подключения сенсора предельно прост – от начала работ до получения первых результатов менее 1 часа
- Результатами работы PT ISIM могут пользоваться как инженеры ИБ, так и специалисты АСУ ТП

PT ISIM View Sensor – поддерживаемые протоколы

POSITIVE TECHNOLOGIES

ПРОМЫШЛЕННЫЕ

- APC FG
- CIP
- DIGSI
- GOOSE
- IEC104
- MMS
- MODBUS TCP
- OPC DA
- PROFINET
- S7 comm
- SPABUS
- UMAS

ОБЩЕСЕТЕВЫЕ

- ARP
- DHCP
- DNS
- FTP
- HTTP
- ICMP
- NTP
- SMB1
- SNMP
- SSH
- TDS
- TELNET
- TFTP

ОБНАРУЖИВАЕМЫЕ

- Ammyy
- Admin
- Bitcoin
- DNP3
- ICQ
- IMAP
- IRC
- JSONRPC
- LLMNR
- MOXACMD
- NBNS
- NFS
- P2P
- Bitmessenger
- POP3
- Quake 1-4
- RADMIN
- RDP
- RTSP
- SIP
- SMTP
- SOCKS5
- SSH
- SYSLOG
- TLS
- TOR
- TeamViewer
- Telegramm
- VNC
- X11
- ZABBIX

POSITIVE TECHNOLOGIES

PT ISTI – Industrial Security Threats Indicators

NOT SNORT- TYPE RULES

GOOSE_Corrupted	Некорректный пакет GOOSE
GOOSE_Unauthorized	Пакет GOOSE от/к неавторизованному узлу
HTTP_Bruteforce	Перебор пароля HTTP (basic-аутентификация)
HTTP_Control_Access	Доступ к веб-интерфейсу устройства
ICMP_Smurf	Попытка вызвать Smurf DDoS
IEC104_Invalid_SQnum	Нарушена последовательность счётчиков IEC104
IEC104_Unknown_IOA	Обнаружено сообщение IEC104 с некорректным адресом объекта
Internet_Detect	Обнаружен доступ в адресное пространство интернет
LLMNR_Unauthorized	Трафик LLMNR с неавторизованного узла
MMS_Cancellation	Отмена операции MMS
MMS_Error	Ошибка MMS
MMS_Rejection	Отказ в сервисе MMS
MMS_Unauthorized_Device_Control	Несанкционированное оперативное переключение коммутационного аппарата
MMS_Unauthorized_Init	Инициировано соединение MMS от неавторизованного узла
MMS_Unauthorized_Write	
MMS_UnauthorizedMMSDa	
MMS_Unknown	
MMS_Unknown_IP	
MMS_Unknown_MAC	
Modbus_Exception	
Modbus_Invalid_Address	
Modbus_Invalid_Count	
Modbus_Invalid_Length	Нестандартная длина пакета Modbus
Modbus_Invalid_Protocol_ID	Нестандартное значение идентификатора протокола Modbus
NBNS_Unauthorized	Пакет NBNS с неавторизованного узла
Network_Scanning	Сканирование сети
NTP_Monlist_DDoS	Атака «отказ в обслуживании» посредством NTP
NTP_Stratum	NTP-сервер слоя 0
OPCDA_Unauthorized_Connection	Взаимодействие по протоколу OPC DA с неавторизованным узлом
OPCDA_Unauthorized_Tag_Writing	Запись значения OPC-тега с неавторизованного узла
Profinet_DCP_Identify_Req_Unauthorized	Запрос идентификации по DCP с неизвестного узла
Profinet_DCP_Identify_Request_Flood	Попытка DOS устройства множественными DCP запросами идентификации

INDUSTRIAL NETWORK SPECIFIC EVENTS

SNORT-TYPE RULES

CVE_2008_2639	Переполнение буфера в CitectSCADA
CVE_2011_4051	Возможно исполнение произвольного кода без авторизации CEServer.exe
CVE_2011_4052	Переполнение буффера CEServer.exe
CVE_2011_4536	Переполнение буфера в WellinTech KingView
CVE_2011_5007	Переполнение буфера в CmpWebServer
FTP_CVE_2014_6271	CVE-2014-6271 (shellshock) посредством FTP
Heartbleed	Heartbleed CVE-2014-0160
HTTP_CVE_2014_6271	CVE-2014-6271 (shellshock) посредством HTTP
MODBUS_CVE_2010_4709	Эксплуатация переполнения буфера Automated Solutions Modbus/TCP Master OPC Server
MODBUS_CVE_2013_0699	Modbus CVE-2013-0699
Snort_Advantech_WebAccess_Dashboard_CVE_2016_0854	Уязвимость загрузки файла Advantech WebAccess Dashboard CVE-2016-0854
Snort_AzeoTech_DAQFactory_Net 3492	
Snort_CVE_2009_4462_Intellicom	
Snort_Measuresoft_ScadaPro_RCE	
Snort_Metasploit_SCADA_Ge_Prot aversal	
Snort_RealWin_SCADA_Srv_DATA verflow	4322
Snort_SCADA_3S_CoDeSys_Srv_Dir_Traversal	Выход в файловую систему сервера SCADA 3S CoDeSys CVE-2012-4705
Snort_Schneider_Accutech_Manager_DoS_CVE_2013_0658	Переполнение буфера URI Schneider Electric Accutech Manager CVE-2013-0658
Snort_Schneider_Electric_Modicon_Discover_Protection_Password	Использование уязвимости CVE-2017-7575
Snort_Sielco_Sistemi_Winlog_BO_CVE_2011_0517	Переполнение буфера Sielco Sistemi Winlog Server Stack CVE-2011-0517
Snort_Triton_Script_Code	TRISIS-TRITON-HATMAN инъекция кода MAR-17-352-01

EXPLOITS ACTIVITIES DETECTION

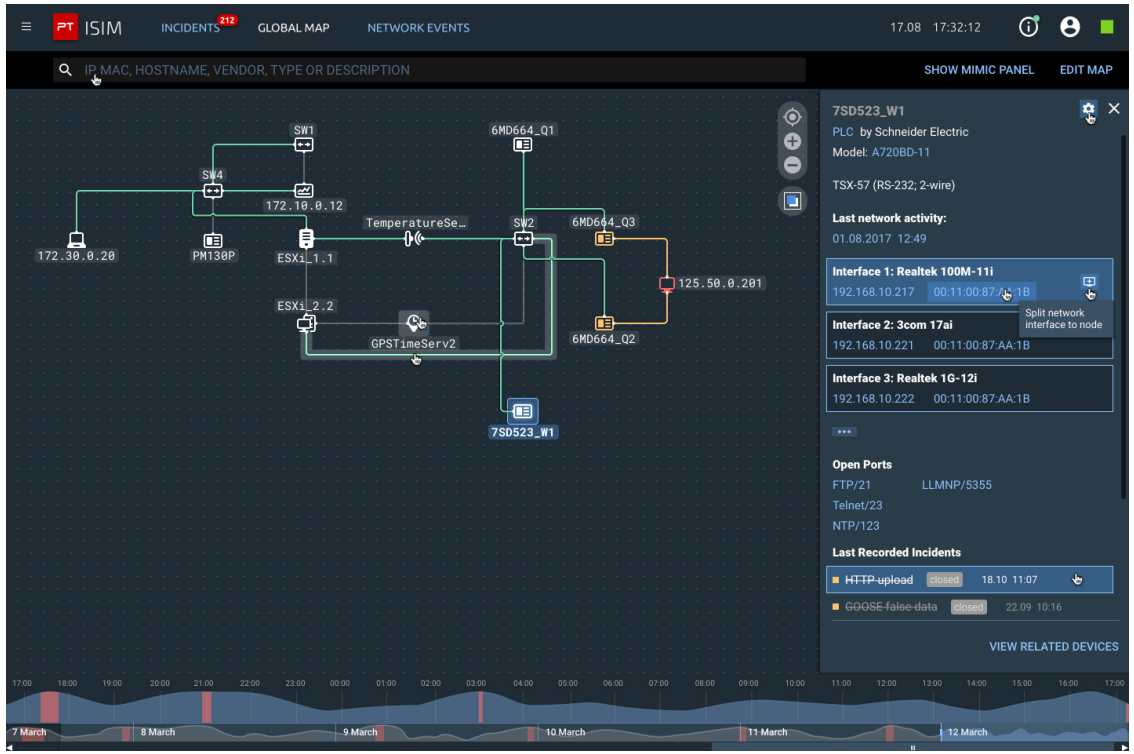
PT ISIM View Sensor – версии

POSITIVE TECHNOLOGIES

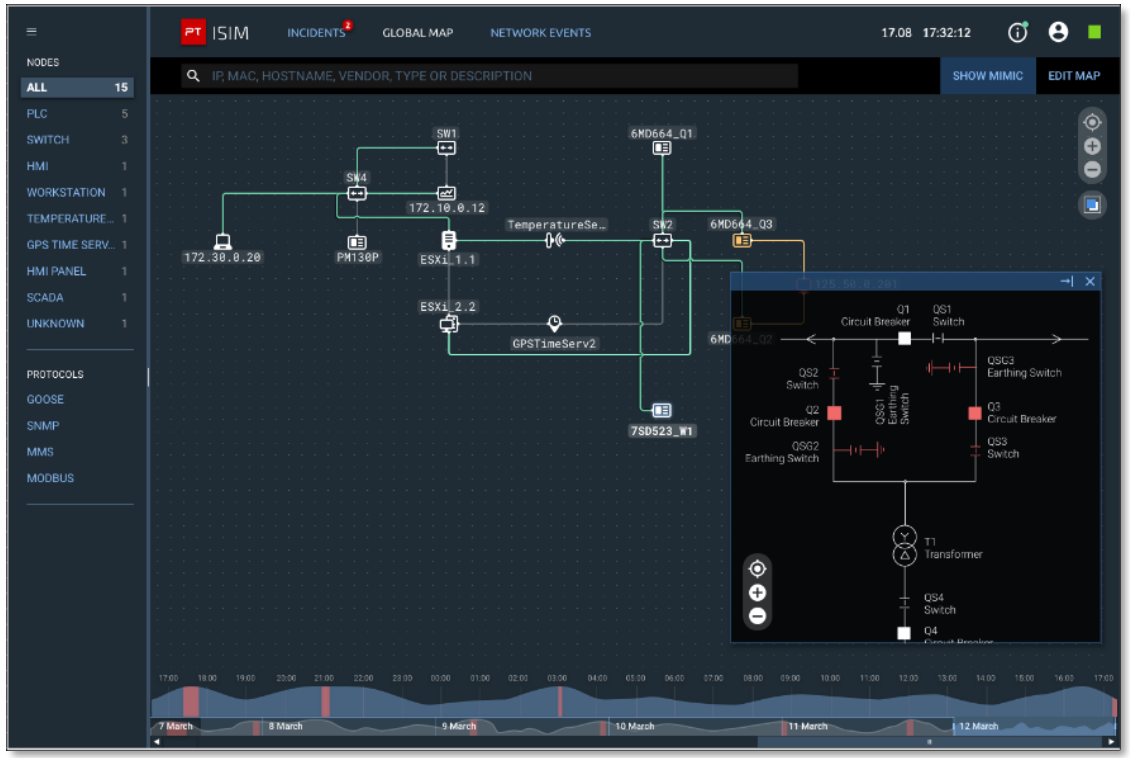
Версия	Ключевые особенности
PT ISIM **net**View Sensor Идеально подходит для большинства предприятий и для задач пилотного внедрения	▪ Работает «из коробки» — автоматически обучается, не требует настройки и специальных знаний ▪ Производит глубокий анализ трафика и инвентаризацию сети АСУ ТП ▪ Позволяет выявить до 80% актуальных угроз сети АСУ ТП ▪ Является уникальным источником информации для анализа инцидентов ИБ ▪ Удобный web-интерфейс
PT ISIM **pro**View Sensor Идеально подходит для компаний со зрелым походом к ИБ АСУ ТП. Требует анализа защищенности АСУ ТП	В дополнение к возможностям версии netView Sensor: ▪ Позволяет тонко настроить механизмы анализа под модель угроз заказчика ▪ Предлагает уникальные опции и инструменты визуализации инцидентов (отображение затронутых атакой элементов на мнемосхеме технологического процесса, индивидуальный интерфейс для инженера АСУ ТП) ▪ Позволяет выявлять сложные многоступенчатые атаки

PT ISIM View Sensor – версии

PT ISIM netView Sensor



PT ISIM proView Sensor



PT ISIM Overview Center - консолидация инцидентов и управление

POSITIVE TECHNOLOGIES

- Консолидация инцидентов с подключенных сенсоров
- Управление жизненным циклом инцидентов
- Централизованное управление сенсорами

Подходит для компаний с распределенной инфраструктурой, а также для интеграторов, предоставляющих услуги коммерческого SOC

PT ISIM Overview Center

- Command center and management
- Hardware appliance

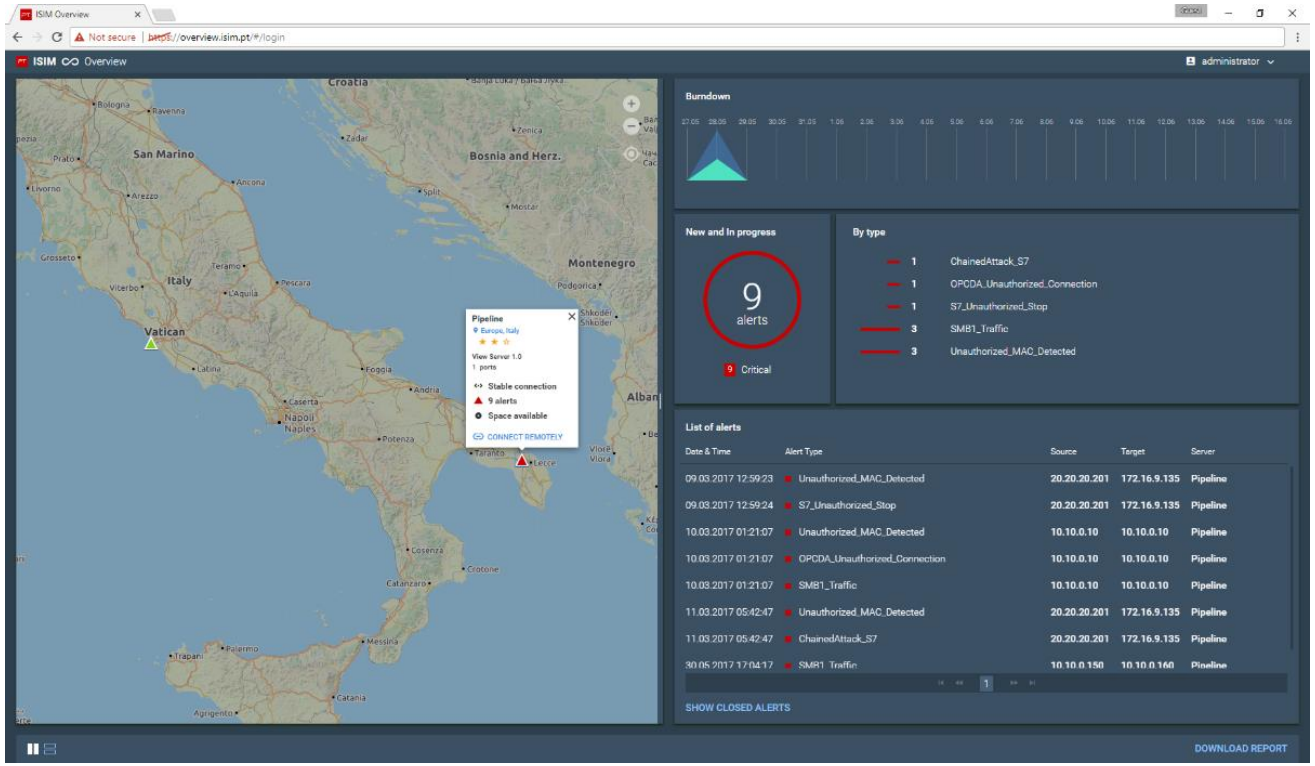
PT ISIM Overview Center – программные компоненты

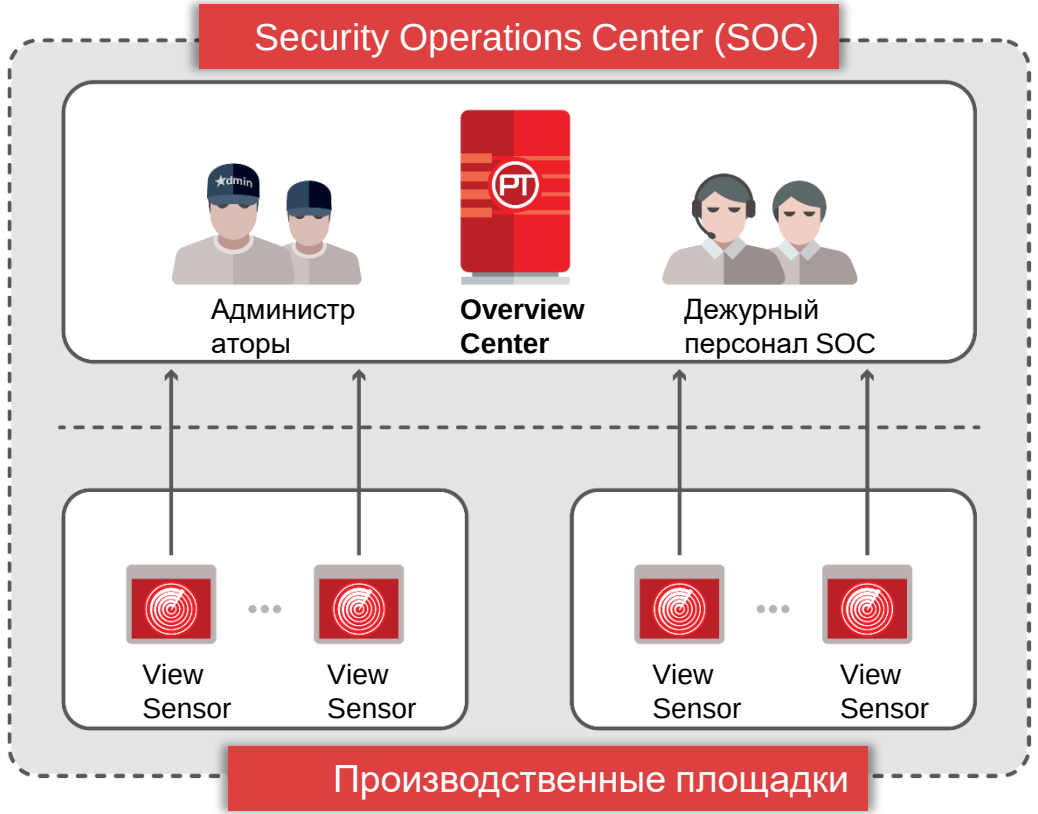
POSITIVE TECHNOLOGIES

Модули ПО	Описание
Business Intelligence	▪ Консолидация информации об инцидентах ▪ Дашборды ▪ Географическая привязка сенсоров ▪ Базовое управление инцидентами
Systems Management	▪ Централизованное управление подключенными сенсорами ▪ Распространение обновлений (ПО сенсоров и база угроз PT ISTI) ▪ Управление лицензиями ▪ Диагностика

PT ISIM Overview Center - консолидация инцидентов и управление

POSITIVE TECHNOLOGIES





POSITIVE TECHNOLOGIES

Thank you!

ptsecurity.com