Платформа кибер-безопасности Palo Alto Networks

Oleksandr Rapp | orapp@paloaltonetworks.com
Системный инженер, Palo Alto Networks

Октябрь 2020

Мировой Лидер Кибербезопасности

95

of Fortune 100

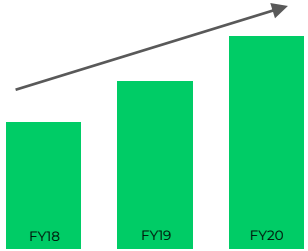
Rely on Palo Alto Networks

71% of the Global 2K
Are Palo Alto Networks Customers

#1

in Enterprise Security

Revenue trend 22% CAGR
FY18 – FY20



18% Year-Over-Year
Revenue Growth

75,000

Customers

In 150+ Countries

5 YEARS IN A ROW
J.D. POWER 2019 CERTIFIED ASSISTED TECHNICAL SUPPORT
2019 tsia RATED OUTSTANDING PALO ALTO NETWORKS | GLOBAL ASSISTED SUPPORT
2015 · 2016 · 2017 · 2018 · 2019

9/10
Average CSAT Score

Gartner, Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q19, 20 March 2020

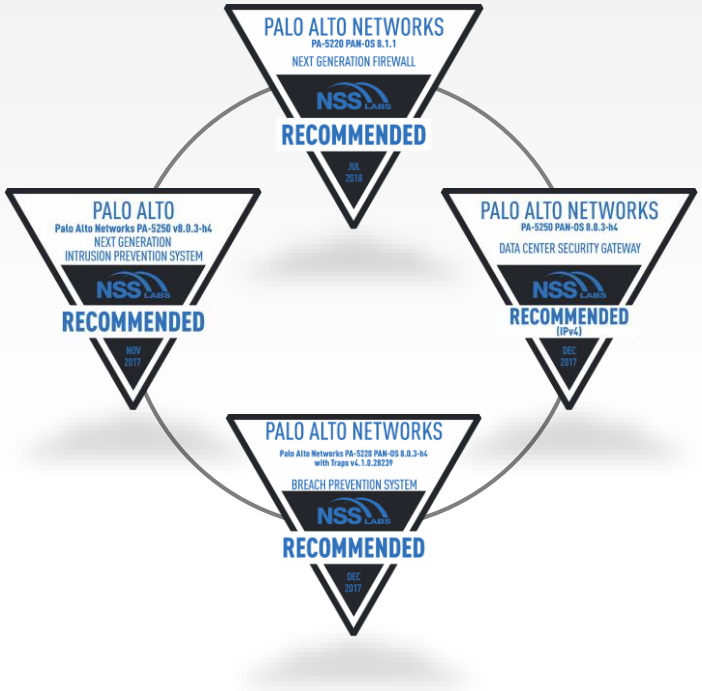
МИРОВОЕ ПРИЗНАНИЕ ВЕДУЩИМИ АНАЛИТИКАМИ И ТЕСТАМИ: NGFW, NGIPS, DataCenter FW и Breach Detection System

Лидер Gartner Magic Quadrant

8 лет подряд

NSS Labs

Рекомендовано по множеству тестов



Лидер в The Forrester Wave™: Enterprise Firewalls Q3’20 Report

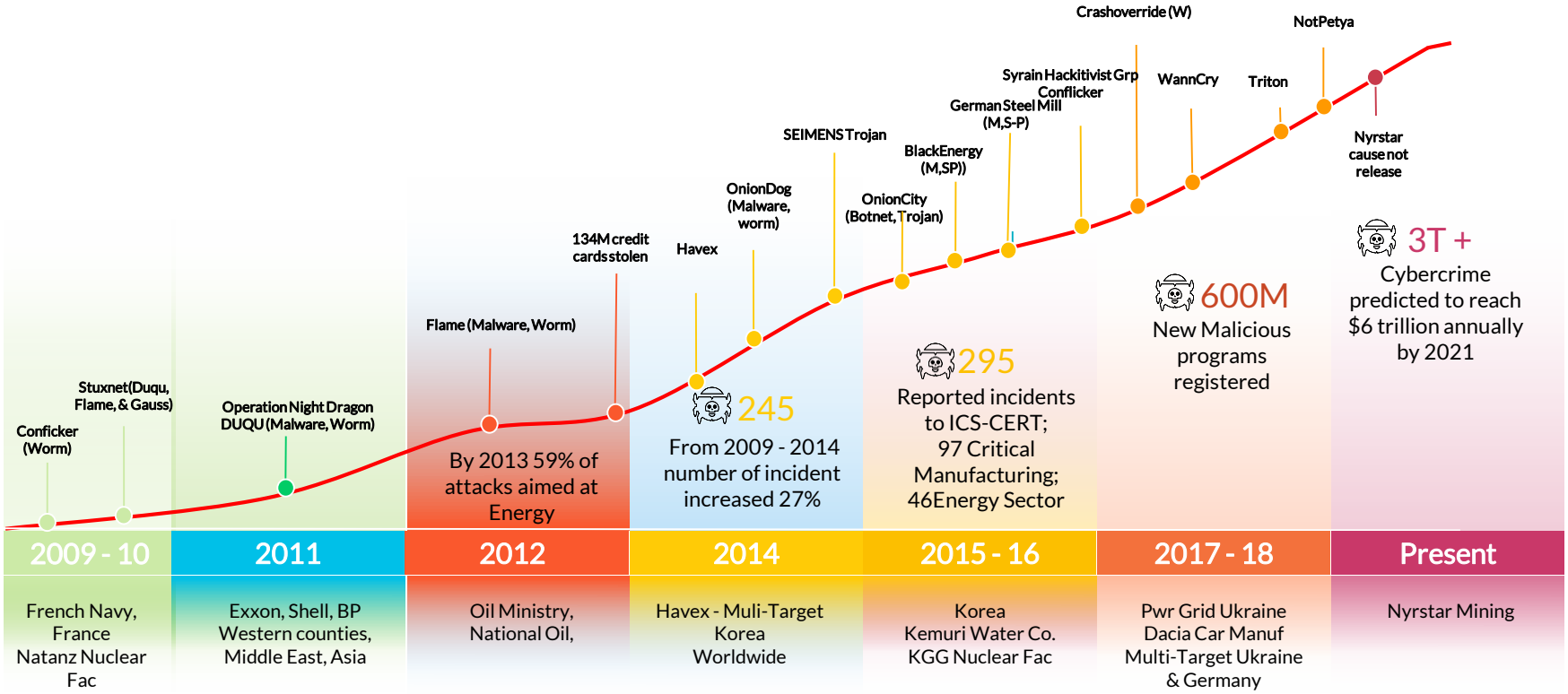
- **Анонсирован ЛИДЕРом в рейтинге** The Forrester Wave™: Enterprise Firewalls Q3 2020 Report
- Получил **наивысшую оценку в категории Стратегия**
- Получил **наивысшую возможную оценку** в 17 критериях, включая **IDS/IPS,** удобство использования, threat intelligence, автоматический анализ зловредного ПО, ICS/OT/IoT

“Enterprise security buyers with a preference for a singl solution vendor should look to Palo Alto Networks to enable their SOC staff and security program.”

--The Forrester Wave™: Enterprise Firewalls Q3’20

Применение NGFW для защиты промышленных (ICS) сетей

Кибер Атаки на Критическую инфраструктуру

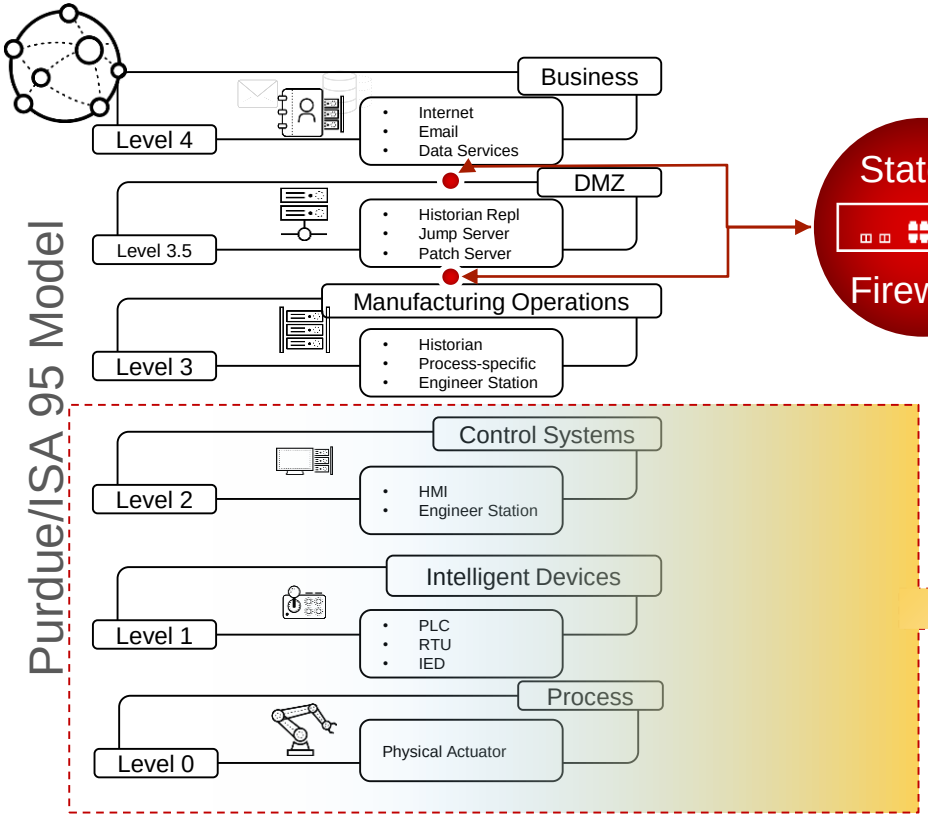


Сложности со Старыми Подходами к Киберзащите в ОТ

Наиболее традиционная Проблема – Плоская сеть

Flat network topologies make it difficult to map to Purdue/ISA95 Model

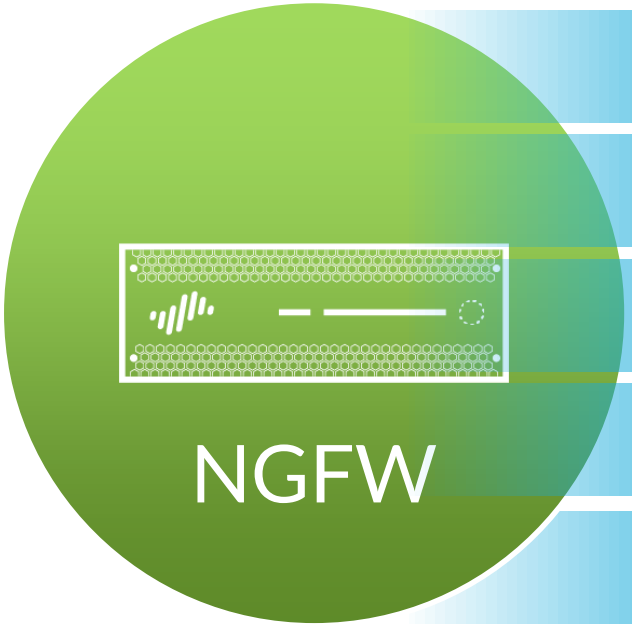
ISA 95/Purdue Model Security Recommendations



Places firewalls in between
- Levels 4 & 3.5
- Levels 3.5 & 3

Design flaw:
Leaves Levels 3 and lower open to attacks that propagate with lateral movement

Что есть в устройстве NGFW



Threat Prevention:	Protect unpatched & unpatchable systems from known & unknown threats to ICS & SCADA
GlobalProtect:	Secure network access for mobile devices in OT E.G. maintenance laptops, tablets, HMIs
Wildfire:	Quickly detect and stop 0-day malware I.E. the next Black Energy, CrashOverride, Wannacry
URL Filtering:	Safely enable internet access from OT E.G. to vendor support website
DNS Filtering:	Safely enable internet access for OT support staff an protect supply chain

IPS сигнатуры для ICS

Product-Specific

Risky Protocol Commands

Iconics Genesis SCADA CSService Integer Overflow Vulnerability

SCADA ICCP Unauthorized MMS Write Request Attempt

Modbus Server Information Fetch Attempt

DNP3 Stop Application Attempt

Galil RIO 47100 PLC

Galil RIO 47100 PLC Denial of Service Vulnerability

Siemens Tecnomatix FactoryLink

IEC-104 Interrogation Command Type-identification Unknown Found

Schneider Electric ClearSCADA

Honeywell OPOS Suite

ID	CVE	Threat Name	Category
31673		SCADA ICCP Unauthorized MMS Write Request Attempt	info-leak
31676		SCADA ICCP COTP Disconnect Protocol Error	info-leak
31651		SCADA Modbus Server Information Fetch Attempt	info-leak
34678		GenBroker SCADA CSService Buffer Overflow Vulnerability	overflow
31677		SCADA ICCP Invalid OSI SSEL Refuse PDU	info-leak
34694		Iconics Genesis SCADA CSService Integer Overflow Vulnerability	overflow
34675		Siemens Tecnomatix FactoryLink SCADA VRN Server M… Vulnerability	overflow
31660		SCADA DNP3 Stop Application Attempt	info-leak
34706		Siemens Tecnomatix FactoryLink SCADA VRN Server Multiple Buffer Overflow Vulnerability	overflow
36944	CVE-2013-0699	Galil RIO 47100 PLC Denial of Service Vulnerability	info-leak
31678		SCADA ICCP Invalid OSI PSEL ACSE Abort Message	info-leak
31662		SCADA DNP3 Broadcast Request Attempt	info-leak
34695		Iconics Genesis SCADA CSService Integer Over…	overflow
		SCADA DNP3 Warm Restart Attempt	info-leak
		Siemens Tecnomatix FactoryLink SCADA VRN Server Multiple Buffer Overflow Vulnerability	overflow
31674		SCADA ICCP Unauthorized MMS Write Request Succeeded	info-leak
34676			
36925	CVE-2011-1564		
		IEC-104 Interrogation Command Information Object Addr… Unknown Found	info-leak
		RealFlex RealWin Buffer Overflow Vulnerability	code-execut…
55034		IEC-104 Interrogation Command Type-identification Unknown Found	info-leak
34696		Iconics Genesis SCADA CSService Integer Overflow Vulnerability	overflow
36983	CVE-2014-0779	Schneider Electric ClearSCADA OPF File Parsing Denial of Service Vulnerability	dos
31670		SCADA ICCP COTP Connection Request from Unauthorized Client	info-leak
		SCADA Modbus TCP server Communications Power Cy… Attempt	info-leak

Примеры приложений для ICS которые видит NGFW

Протокол / приложение	Протокол / приложение	Протокол / приложение	Протокол / приложение	Протокол / приложение
■ DNP3 **(DECODER)**	■ Modbus**(DECODER)**	■ Siemens S7**(DECODER)**	■ Schneider/Wonderware SuiteLink	■ Fisher-ROC
■ IEC 60870-5-104**(DECORDER)**	■ CIP EtherNet IP**(DECODER)**	■ Siemens FactoryLink	■ Schneider OaSys	■ Cygnet SCADA
■ ICCP (IEC 60870-6 / TASE.2) **(DECODER)**	■ BACnet **(DECODER)**	■ Siemens Profinet IO	■ Rockwell FactoryTalk	■ Fanuc-Focas
■ Synchrophasor (IEEE C.37.118)	■ OPC UA	■ ABB Network Manager	■ GE iFIX	■ MQTT
■ Elcom 90	■ OPC DA	■ Honeywell/Matrikon OPC Tunneller	■ GE EGD	■ RTCM (GPS/IP)
■ DLMS / COSEM / IEC 62056 ■ MMS-ICS ■ CC-Link	■ R-GOOSE ■ IEC 61850**(DECODER)**	■ OSIsoft PI Systems ■ Cygnet SCADA	■ GE-Historian ■ Schweitzer Engineering SEL Fast Messaging	■ ADDP ■ COAP ■ 104 APCI

- Основные App-ID приложения
- Распознавание неизвестных: Unknown TCP , Unknown UDP
- Функции приложений в App-IDs: Modbus, DNP3, ICCP, S7, BACnet, IEC 60870-5-104, IEC 61850, CIP-EtherNet-IP
- Кастомные App-ID декодеры для ICS: Modbus, ICCP, DNP3
- Запрос на новые App-ID в онлайн

http://researchcenter.paloaltonetworks.com/submit-an-application/

Более точный контроль функций в каждом ICS протоколе

MODBUS

- modbus
  - modbus-base
  - modbus-write-multiple-coils
  - modbus-write-file-record
  - modbus-read-write-register
  - modbus-write-single-coil
  - modbus-write-single-register
  - modbus-write-multiple-registers
  - modbus-read-input-registers
  - modbus-encapsulated-transport
  - modbus-read-coils
  - modbus-read-discrete-inputs
  - modbus-mask-write-register
  - modbus-read-fifo-queue
  - modbus-read-file-record
  - modbus-read-holding-registers

DNP3

- dnp3
  - dnp3-base
  - dnp3-write
  - dnp3-read
  - dnp3-operate
  - dnp3-direct-operate
  - dnp3-confirm
  - dnp3-record-current-time
  - dnp3-open-file
  - dnp3-close-file
  - dnp3-delete-file
  - dnp3-get-file-information
  - dnp3-authenticate-file
  - dnp3-abort-file
  - dnp3-freeze-at-time
  - dnp3-freeze-at-time-no-resp
  - dnp3-cold-restart
  - dnp3-warm-restart
  - dnp3-initialize-data
  - dnp3-initialize-application
  - dnp3-select
  - dnp3-direct-operate-no-resp
  - dnp3-freeze
  - dnp3-freeze-no-resp
  - dnp3-freeze-clear-no-resp
  - dnp3-start-application
  - dnp3-stop-application
  - dnp3-save-configuration
  - dnp3-enable-unsolicited
  - dnp3-disable-unsolicited
  - dnp3-assign-class
  - dnp3-delay-measurement
  - dnp3-freeze-clear

ICCP

- iccp
  - iccp-base
  - iccp-read
  - iccp-define-named-type
  - iccp-define-named-variable
  - iccp-define-named-variable-list
  - iccp-define-scattered-access
  - iccp-define-semaphore
  - iccp-delete-named-type
  - iccp-delete-named-variable-list
  - iccp-delete-semaphore
  - iccp-delete-variable-access
  - iccp-download-segment
  - iccp-get-named-type-attr
  - iccp-get-named-var-list-attr
  - iccp-get-name-list
  - iccp-get-scattered-access-attr
  - iccp-get-variable-access-attr
  - iccp-identity
  - iccp-initiate-download-seq
  - iccp-initiate-upload-seq
  - iccp-input
  - iccp-output
  - iccp-relinquish-control
  - iccp-rename
  - iccp-report-pool-sem-status
  - iccp-report-semaphore-status
  - iccp-report-sem-entry-status
  - iccp-status
  - iccp-take-control
  - iccp-terminate-download-seq
  - iccp-write

BACnet

- bacnet
  - bacnet-base
  - bacnet-ack-alarm
  - bacnet-confirmed-cov-notify
  - bacnet-confirmed-event-notify
  - bacnet-get-alarm-summary
  - bacnet-get-enrollment-summary
  - bacnet-subscribe-cov
  - bacnet-atomic-read-file
  - bacnet-atomic-write-file
  - bacnet-add-list-element
  - bacnet-remove-list-element
  - bacnet-create-object
  - bacnet-delete-object
  - bacnet-read-property
  - bacnet-read-prop-conditional
  - bacnet-read-prop-multiple
  - bacnet-write-property
  - bacnet-write-prop-multiple
  - bacnet-device-comm-control
  - bacnet-confirmed-private-xfer
  - bacnet-confirmed-text-message
  - bacnet-reinitialize-device
  - bacnet-vt-open
  - bacnet-vt-close
  - bacnet-vt-data
  - bacnet-authenticate
  - bacnet-request-key
  - bacnet-read-range
  - bacnet-life-safety-operation
  - bacnet-subscribe-cov-property
  - bacnet-get-event-information

S7

- siemens-s7
  - siemens-s7-base
  - siemens-s7-read
  - siemens-s7-stop
  - siemens-s7-start
  - siemens-s7-setup-communication
  - siemens-s7-check-password-set
  - siemens-s7-status-controller

IEC “104”

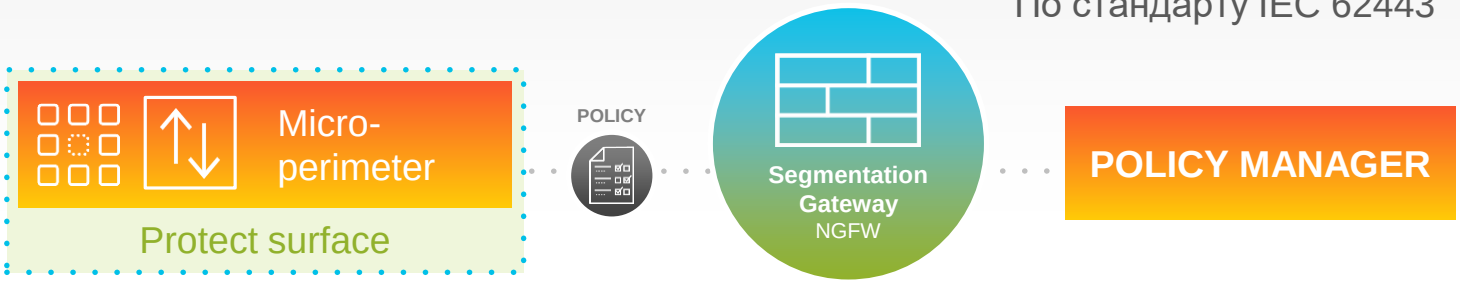
- iec-60870-5-104
  - iec-60870-5-104-base
  - 104asdu-process-monitor
  - 104asdu-process-control
  - 104asdu-system-monitor
  - 104asdu-system-control
  - 104asdu-param-control
  - 104apci-supervisory
  - 104apci-unnumbered
  - 104asdu-file-transfer

Можно сегментировать сети в самом NGFW

- Максимальная визуализация трафика между OT, IT, IoT и IIoT traffic.
- Контроль всех доступов.
- Блокировка известных вирусов, эксплойтов и систем управления бот-сетями
- Быстро распознает zero—day в OT и IT инфраструктуре

Почему сегментация?
Задать площади для контроля

Как происходит сегментация?
На уровнях 1-7
По стандарту IEC 62443



Industrial Cybersecurity Partnerships

Siemens Plant Security Services Webpage

- Link

Industry Online Support Denmark | Contact | Help | Support Request

Home > Product Support

Entry type: **Product note**, Entry ID: **109753709**, Entry date: **12/12/2017**

☆☆☆☆☆ (0)
> Rate

Plant Security Services released Perimeter Firewall Installation including Next Generation Firewall for Sales and Delivery

Entry | Associated product(s)

Plant Security Services released Perimeter Firewall Installation including Palo Alto Networks' Next Generation Firewall for Sales and Delivery

1. **Product description**

The portfolio element Perimeter Firewall Installation as part of the cluster Implement Security enhances the Plant Security Portfolio with an element that helps to segment and protect the industrial networks from threats coming from the outside. This is an integral part of the defense in depth concept of the IEC 62443.

a. **Perimeter Firewall Installation**

Installation and configuration of Perimeter Firewall within an automation plant. Pricing includes configuration of firewall rules with direct 1-to-1 relationship to existing firewall rules or design of maximum 40 new firewall rules.

Perimeter Firewall Installation consists of the following:

- Review of plant network layout
- Creation of a Plant Perimeter Firewall concept. This is established in collaboration with the customer and includes the definition of IDS settings, deployment model, alerting settings, communication matrix and other firewall specific settings.
- Installation and configuration of Perimeter Firewall with 1-1 implementation of existing firewall rules implemented on previous plant perimeter firewall device on plant perimeter or design of maximum 40 new firewall rules, if no firewall will be replaced
- Test of communication via the Plant Perimeter Firewall in collaboration with the customer
- Perimeter Firewall Installation Report delivery

b. Palo Alto Networks PA-220 Next-Generation Firewall

(Support must be purchased separately!)

Performance and Capacities	-	PA-220
Firewall throughput (App-ID)	-	500 Mbps
Threat prevention throughput	-	150 Mbps
IPsec VPN throughput	-	100 Mbps
New sessions per second	-	4.200
Max sessions	-	64.000

c. Palo Alto Networks PA-800 Series Next-Generation Firewall

(Support must be purchased separately!)

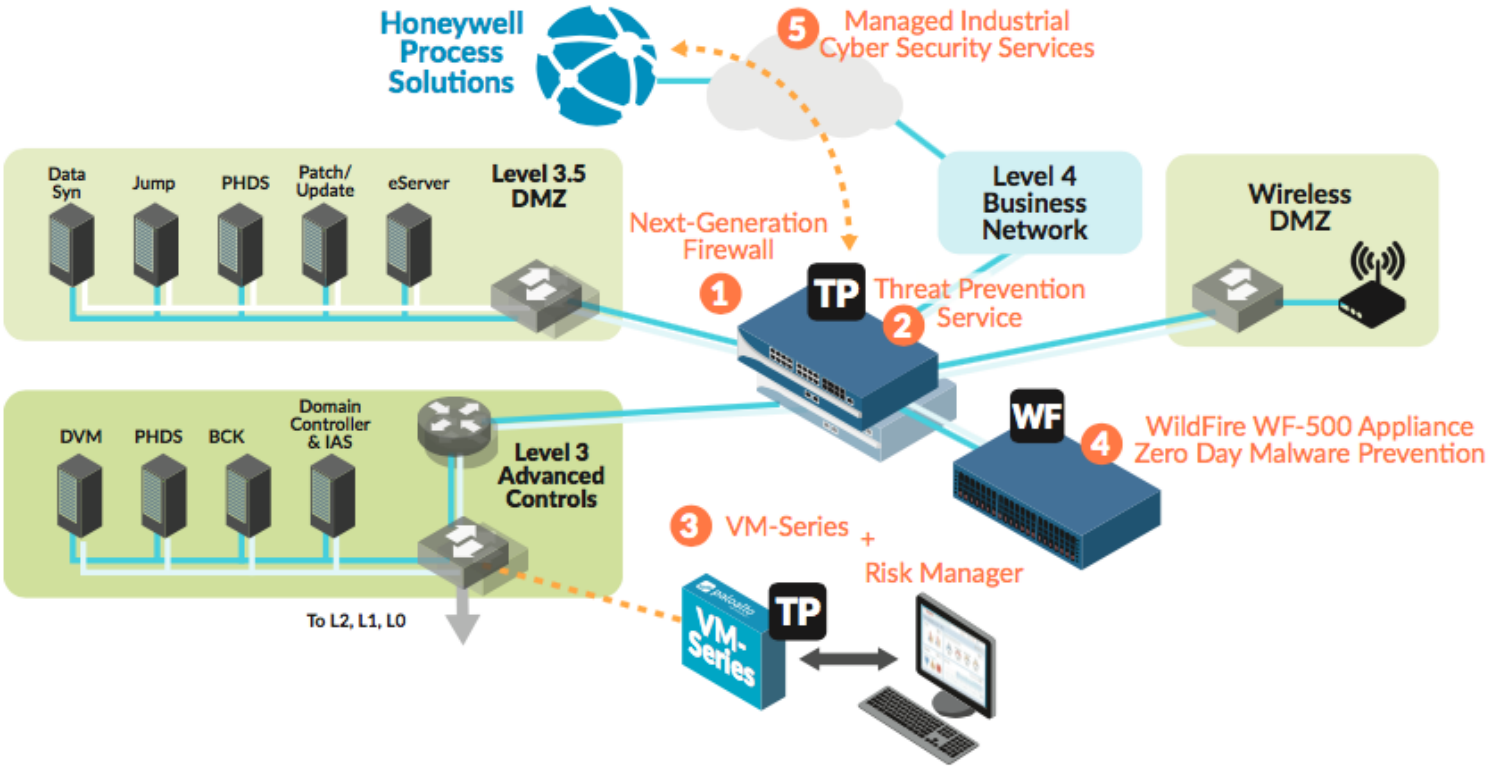
Performance and Capacities	PA-850	PA-820
Firewall throughput (App-ID)	1,9 Gbps	940 Mbps
Threat prevention throughput	780 Mbps	610 Mbps
IPsec VPN throughput	500 Mbps	400 Mbps
New sessions per second	9.500	8.300
Max sessions	192.000	128.000

d. Palo Alto Networks PA-3020 Next-Generation Firewall

(Support must be purchased separately!)

Performance and Capacities	-	PA-3020
Firewall throughput (App-ID)	-	2 Gbps
Threat prevention throughput	-	1 Gbps
IPsec VPN throughput	-	500 Mbps
New sessions per second	-	50.000
Max sessions	-	250.000

ICS Partnerships – Honeywell Joint Reference Architecture



CORTEX
BY PALO ALTO NETWORKS

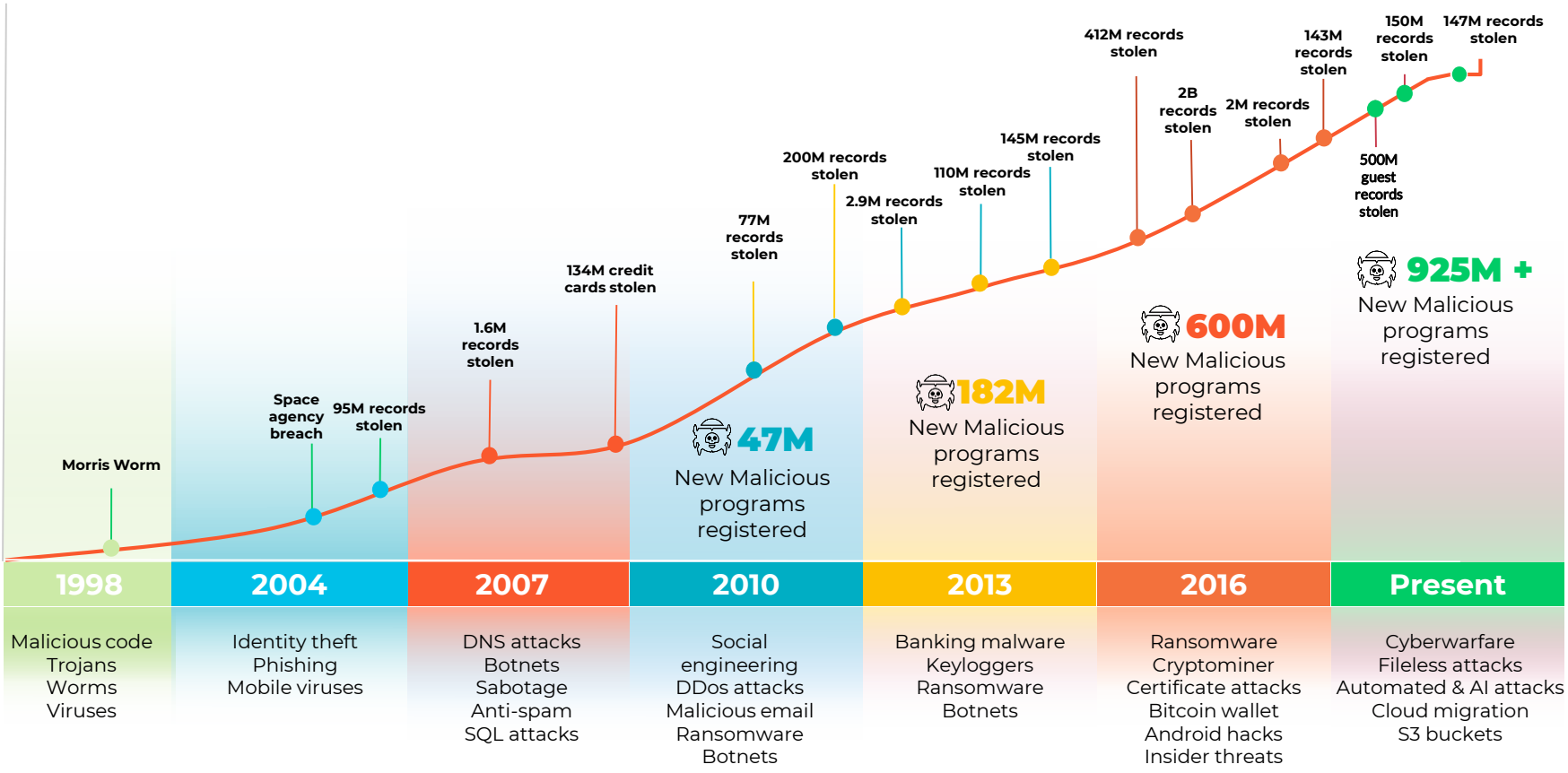
Автоматизация SOC с помощью Cortex XSOAR

Олександр Рапп | orapp@paloaltonetworks.com
Системный инженер | Palo Alto Networks

Октябрь 2020

paloalto NETWORKS

Угрозы становятся сложнее и изощреннее



Проблематика

Реальная угроза для бизнеса / гос предприятий — злоумышленники, обладающие высокой квалификацией в области информационных технологий и владеющие различными методами взлома. Именно они способны реализовать сложные атаки на IT-инфраструктуру с помощью:

- Массовых атак (Notpetya, Wannacry)
- Целевых атак (RSA Security, Sony, Олимпийские игры в Пхенчхане, Garmin и т.д.)

Проблема в том, что квалифицированные злоумышленники способны обойти *любые средства безопасности*. Причем, как показывает практика, зачастую компании узнают о взломе уже после того, как наступили последствия — украдена информация, оказались зашифрованы данные, злоумышленники потребовали выкуп или, находясь в инфраструктуре несколько месяцев, подготовились и в какой-то момент вывели большую сумму денег.

Любой этап атаки должен фиксироваться как инцидент ИБ. Выявляет инциденты на ранних этапах атаки центр мониторинга ИБ и реагирования на инциденты — **security operations center** (SOC). В его задачи входят

- контроль активности в IT-инфраструктуре,
- анализ событий,
- обнаружение угроз ИБ и реагирование на них.

В основе SOC всегда выделяют три составляющие — технологии, люди и процессы.

Терминология SOC

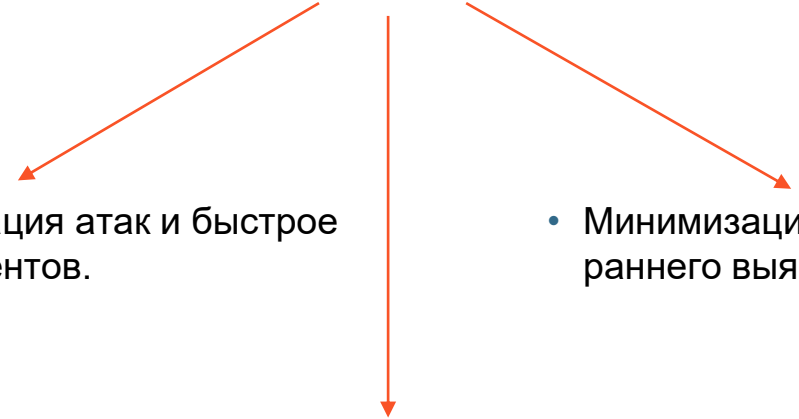
- SOC (**Security Operations Center**), **Центр оперативного реагирования на инциденты ИБ** – это организационная единица подразделения информационной безопасности, объединяющая в себе людей, процессы и технологии, предназначенные для получения ситуационной осведомлённости в процессе обнаружения, локализации и предотвращения угроз информационной безопасности.

- SOC представляет собой эволюцию понятия CERT (Computer Emergency Response Team) – группу реагирования на чрезвычайные ситуации в области IT технологий – Одно из ключевых отличий – использование аналитических технологий для создания единого оперативного видения текущей ситуации в компании с точки зрения ИБ. “Стеклянная кабина” для самолёта информационной безопасности.

Традиционно понятие SOC имеет множество наименований. Только в английском языке это:
- security defense center;
- security analytics center;
- security intelligence center;
- cyber security center;
- threat defense center,
- security intelligence and operations center

Преимущества SOC

Центр Оперативного Реагирования



- Ранняя идентификация атак и быстрое разрешение инцидентов.
- Минимизация финансовых потерь за счет раннего выявления инцидентов
- Устранение инцидентов до их влияния на продуктив.

Основные технологии, используемые SecOps

- Next Generation Firewalls
- Endpoint Protection Platforms (Anti-Viruses)
- Endpoint Detection and Response (EDR, Forensics) – Cortex XDR
- Threat Intelligence Feeds
- Sandboxing
- System Incident and Event Manager (SIEM)
- Networks Traffic Analysis (NTA)
- User and Entity Behavioral Analysis (UEBA)
- Почтовые системы
- Active Directory
- И много других

Проблемы отделов безопасности

Количество уведомлений растет

Слишком много событий ИБ

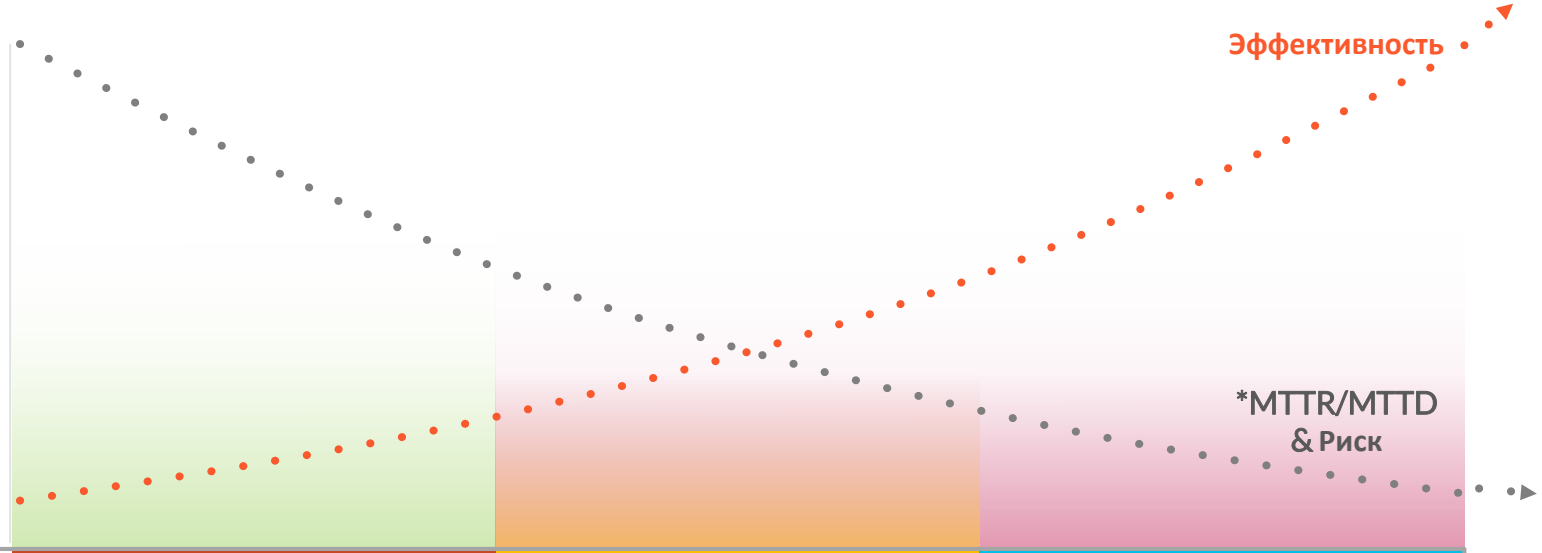
Времени не хватает

Много рутины (проверить все hash на VT и др.)

Ограниченный контекст

Мало информации по инцидентам, много времени на расследование

Как SOC должен изменяться что бы снизить риски

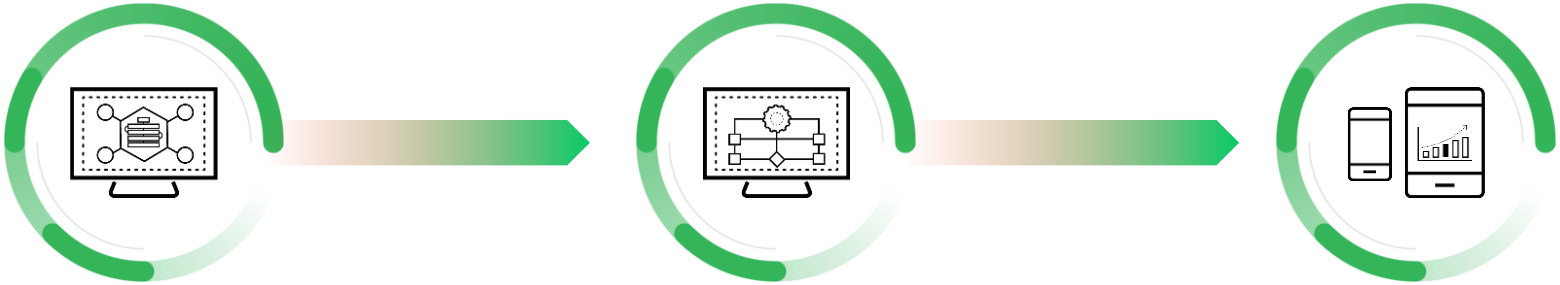


Зрелость	Низкая (Реактивная)	Средняя	Высокая (Проактивная)
Обнаружение	На основе правил	Корреляционные правила	На основе анализа
Контекст	Агрегация логов	Раздельный сбор данных	Интегрированные «обогащённые» данные
Автоматизация	Никакой	Частично	Полностью

*MTTR – mean time to respond – среднее время реагирования
MTTD – mean time to detect – среднее время обнаружения

Что такое SOAR?

Security **O**rchestration, **A**utomation, and **R**esponse



Orchestration

Интеграция и оркестрация с продуктами ИБ и не только

Automation

Автоматизация рутинных процессов

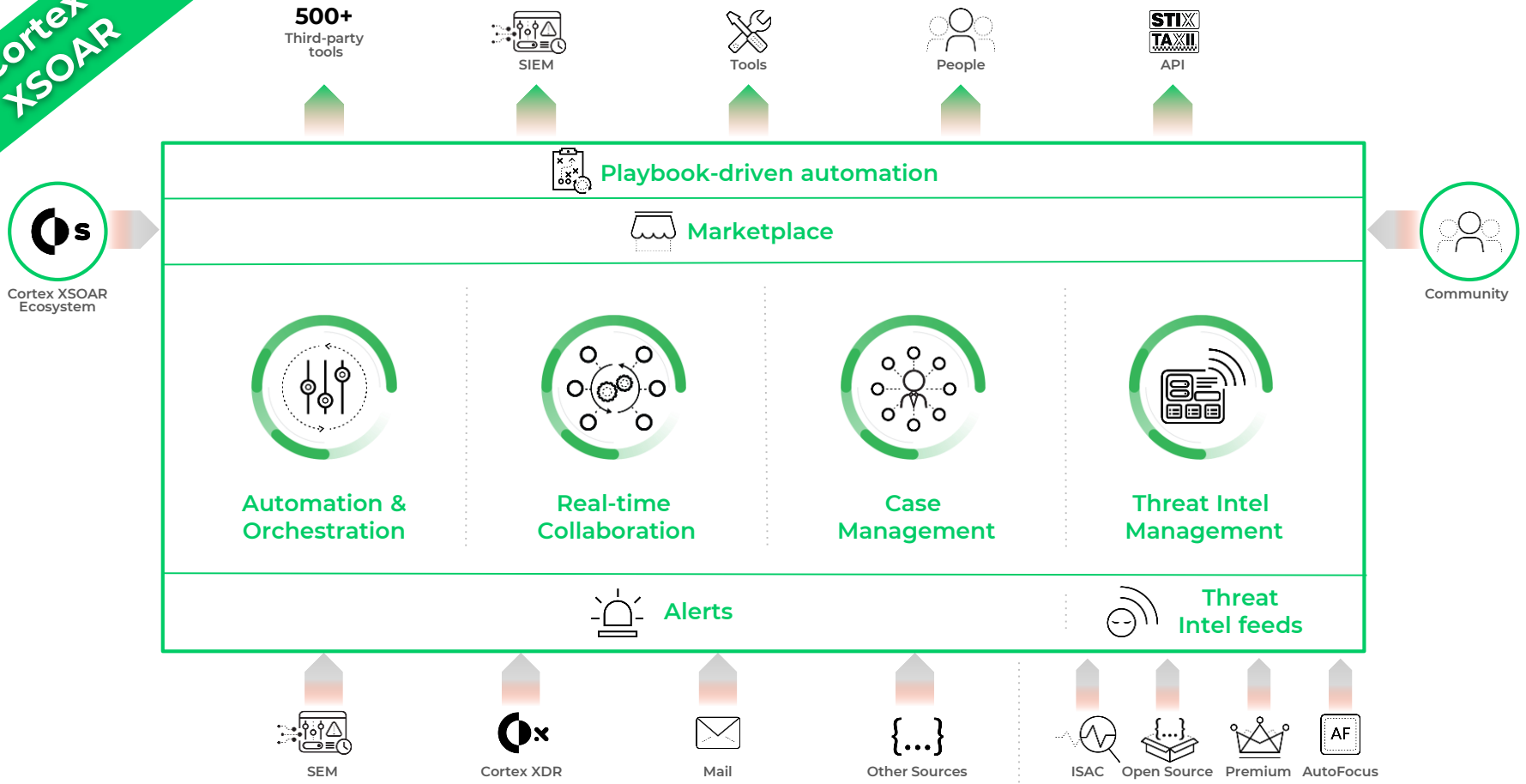
Множество готовых шаблонов

Response

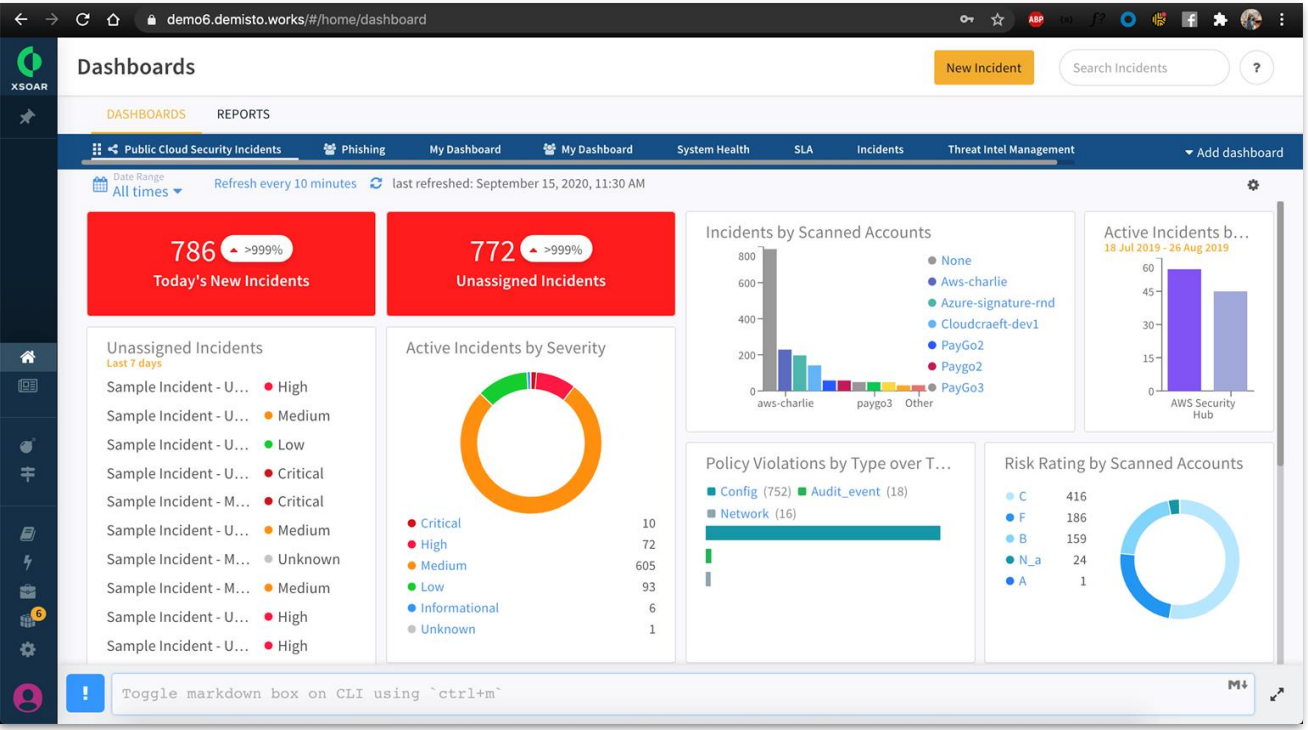
Инцидент менеджмент

(автоматическое создание инцидентов, графическое управление, отчетность)

Cortex XSOAR



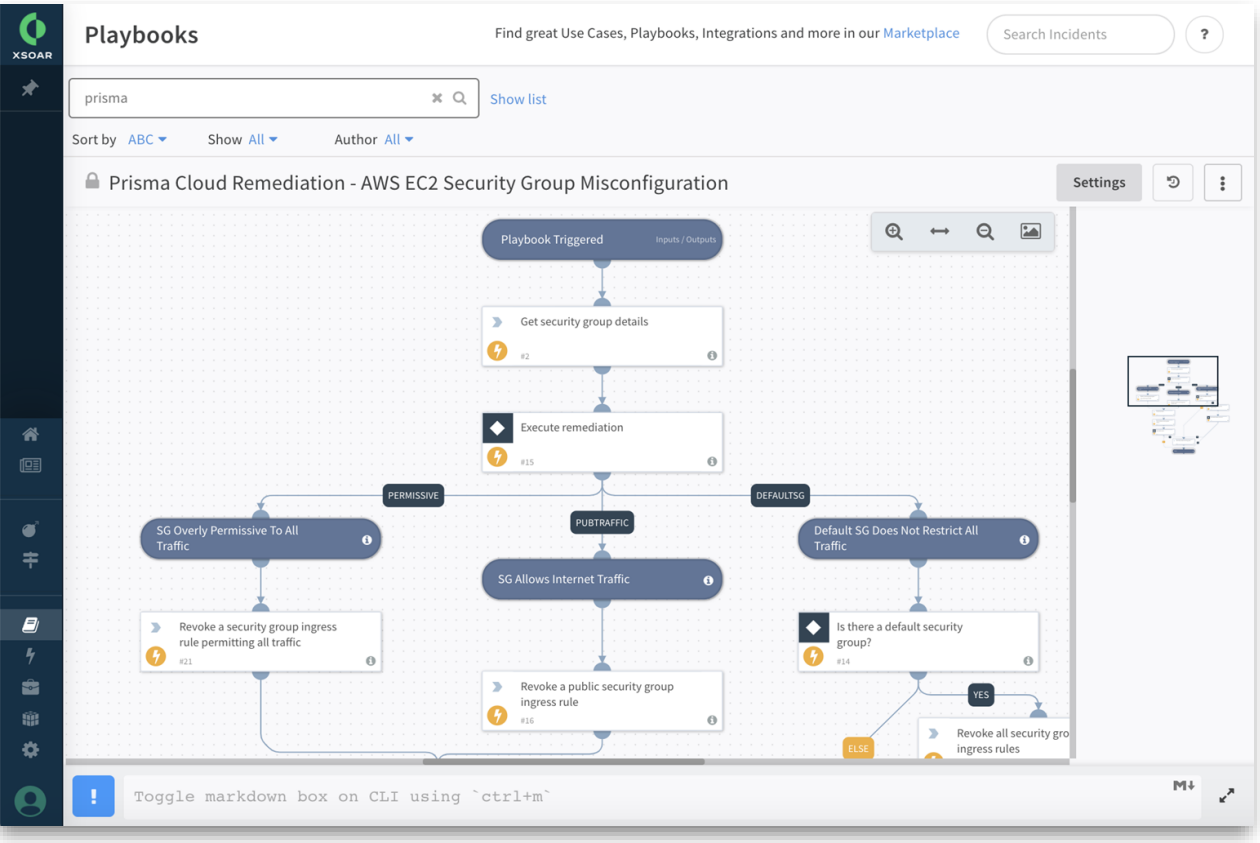
 |



Cortex XSOAR - это система обработки инцидентов

Стандартизация процессов работы для продуктов, команд и различных юз кейсов

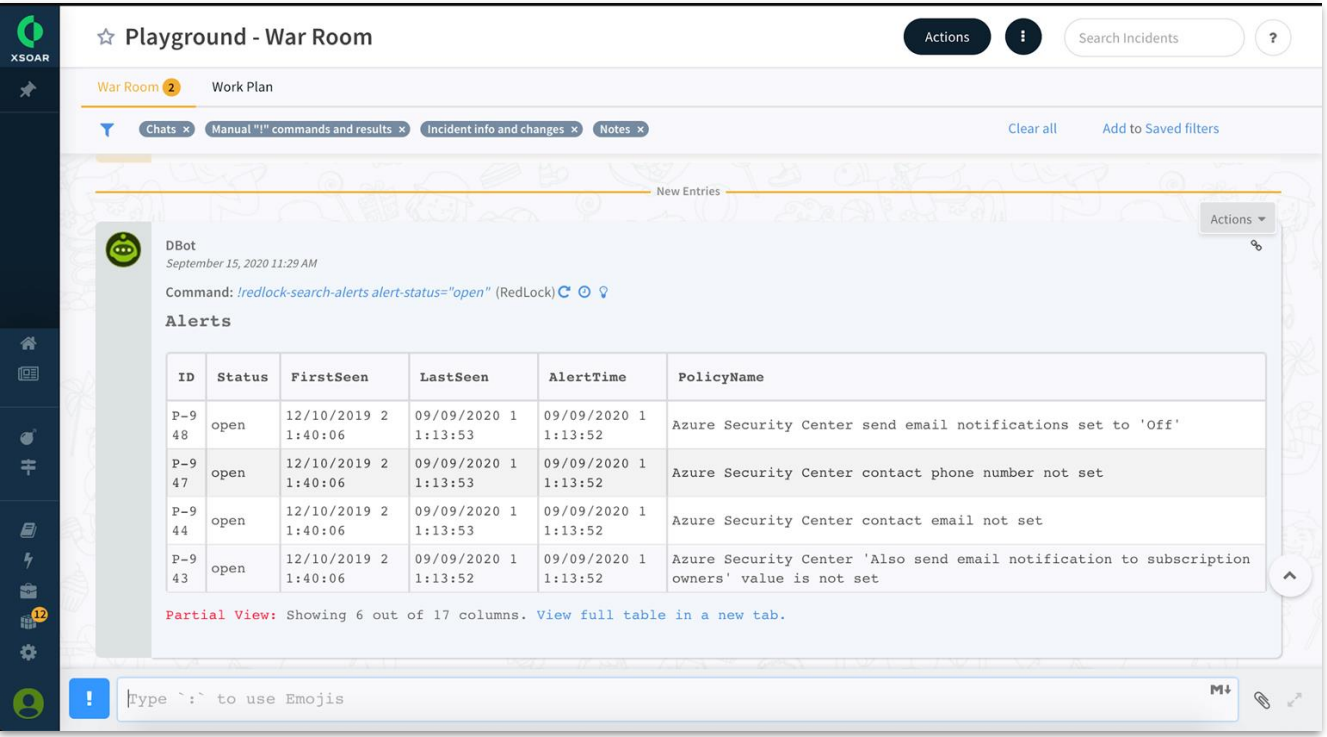
- Получение **ВСЕХ** алертов безопасности и поиск по ним
- Настраиваемые **дашборды** и **отчетность**



Cortex XSOAR это дви жок автоматизации процедур (workflow)

Быстрая и масштабиро-ванная реакция на инциденты безопасности

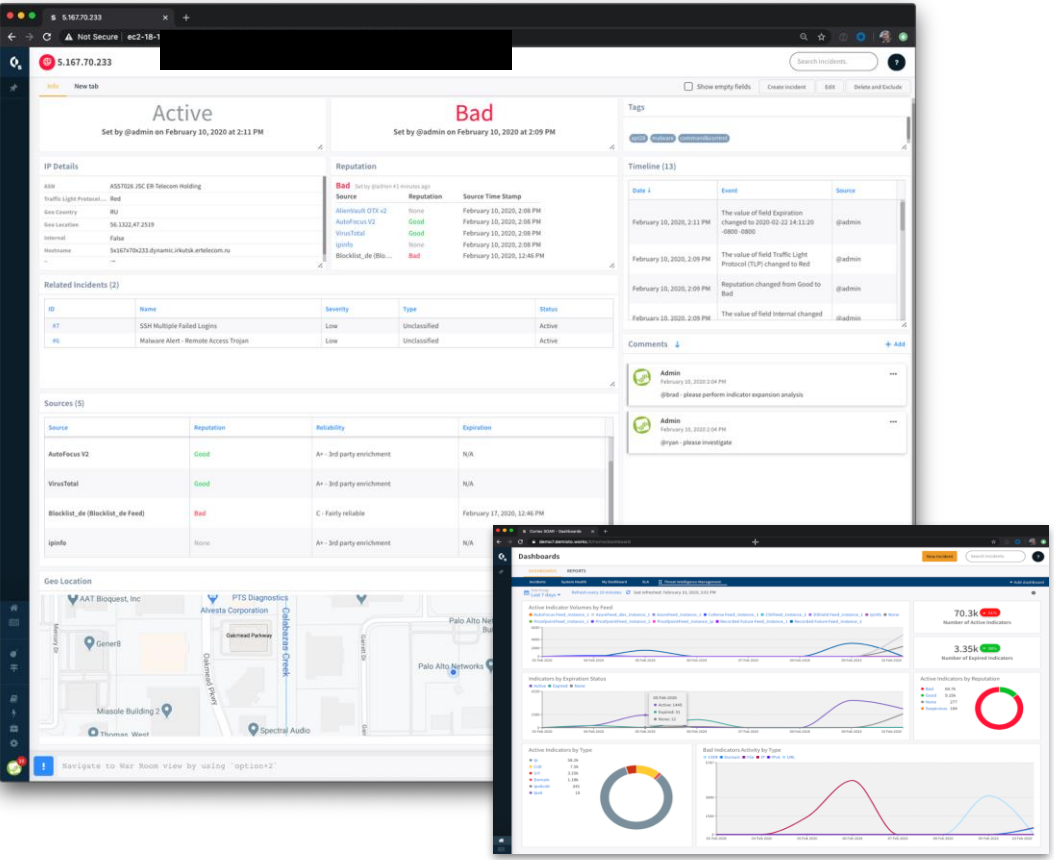
- **100и** интеграций продуктов
- **1000и** автоматизаций
- Интуитивный, **визуальный редактор плейбуков**



Cortex XSOAR – это платформа взаимодействия

Улучшение качества расследования при совместной работе

- **Virtual War Room** для каждого инцидента
- **ChatOps &** действия **в режиме реального времени**
- **Авто-документация** действий в режиме реального времени



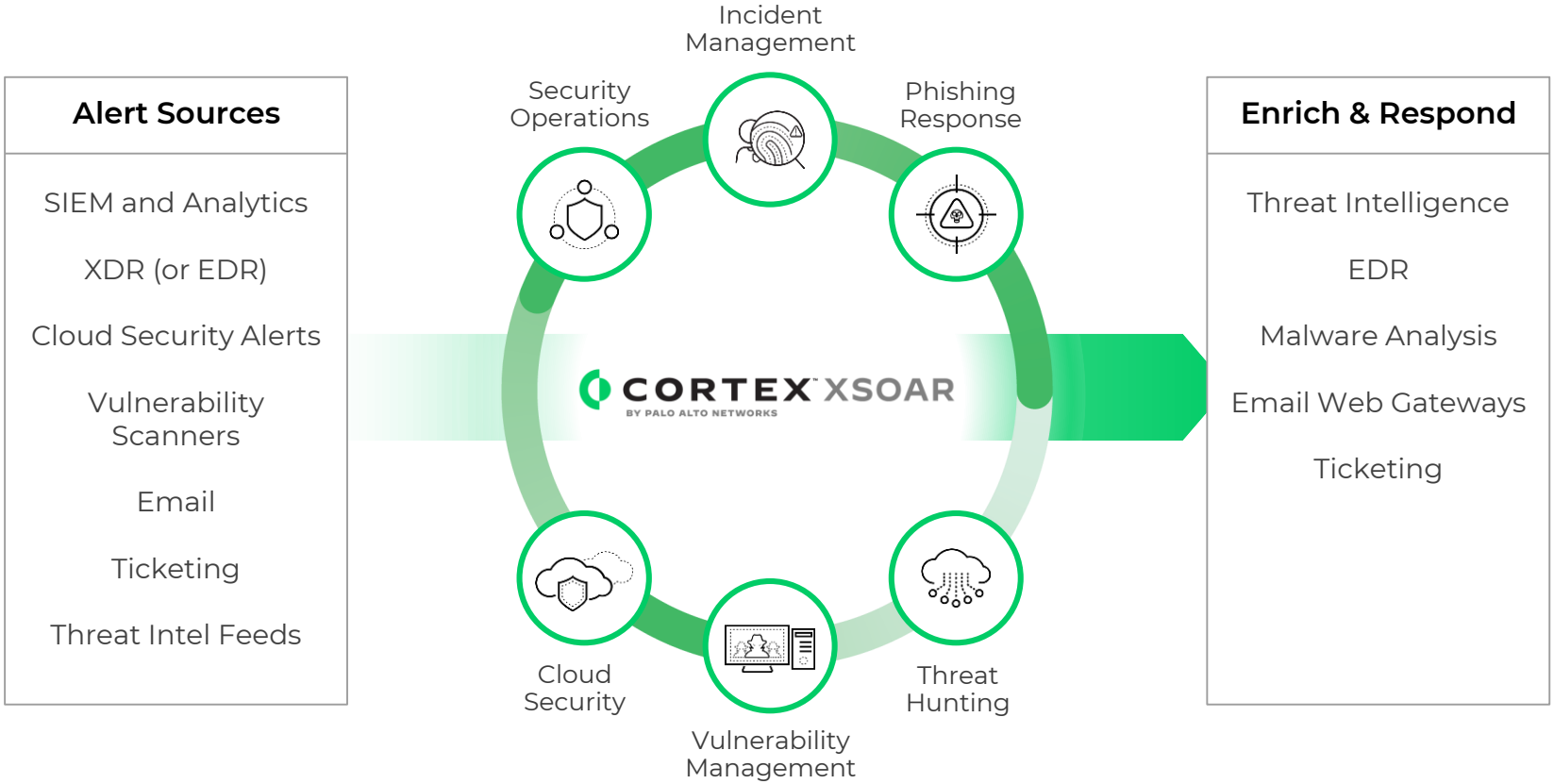
Cortex XSOAR это threat intel management платформа

Возьмите полный контроль над вашими threat intel фидами

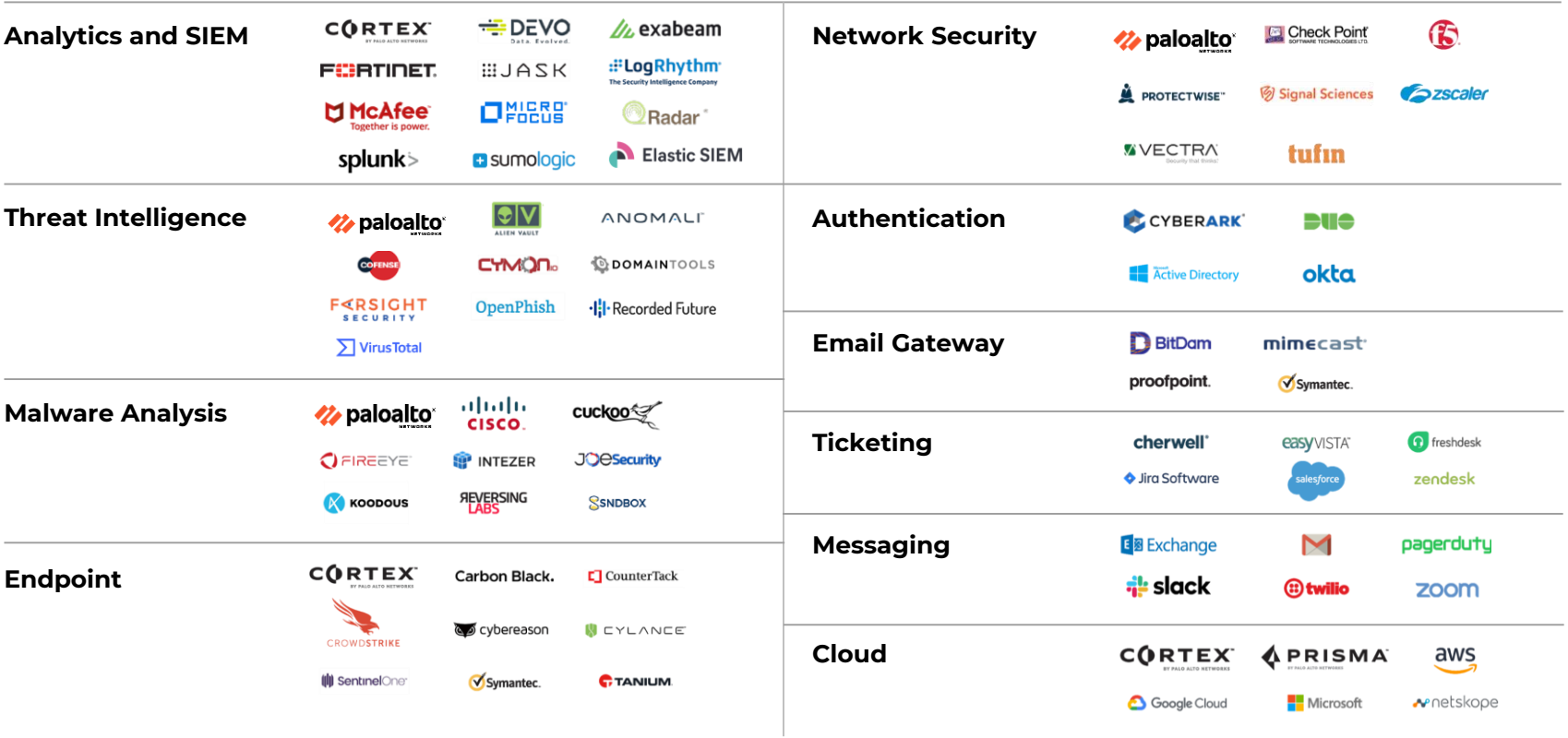
- **Автоматизация** ежедневных повторяющихся действий с индикаторами
- **Получите мгновенную окупаемость инвестиций** от существующих threat intel фидов
- **Будьте уверены** в каждом решении при реагировании на инциденты

 |

Множество различных сценариев применения Cortex XSOAR

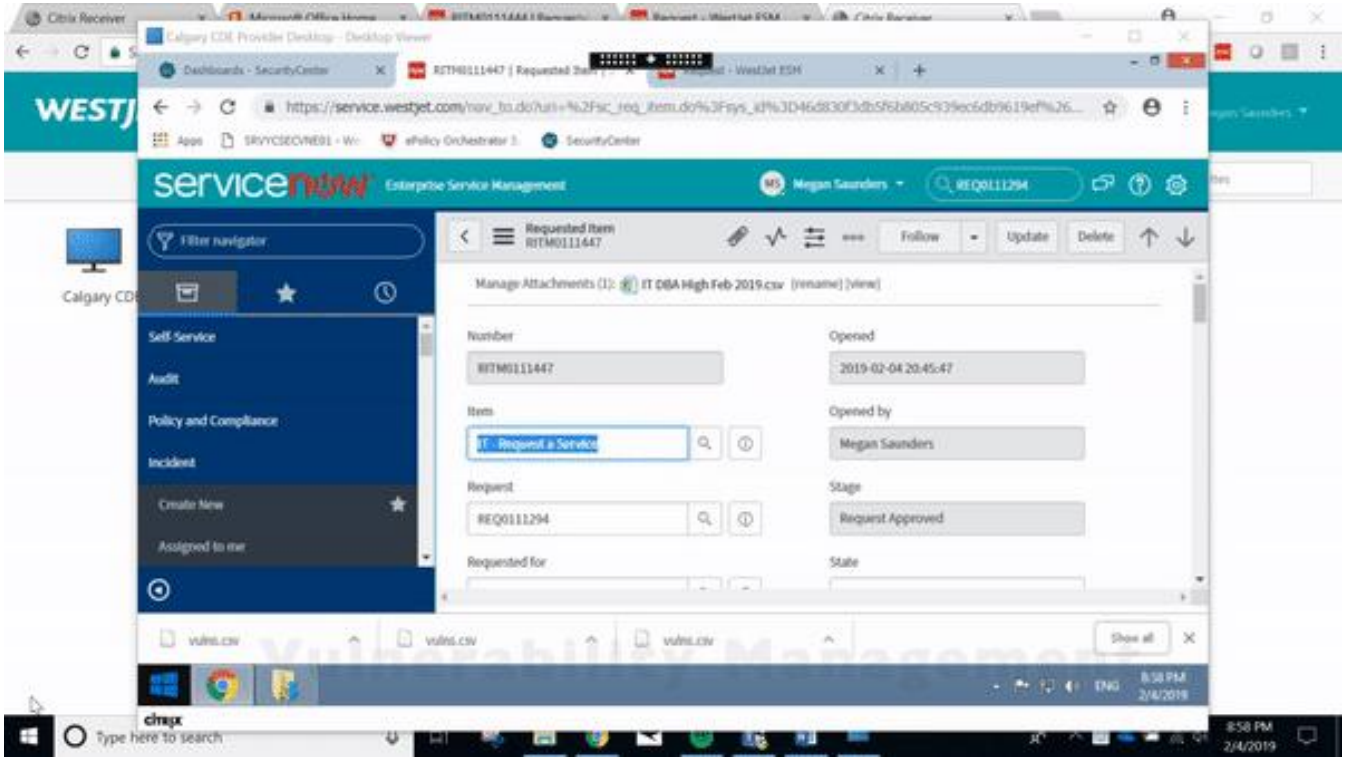


Cortex XSOAR Экосистема (500+ Интеграций)



Пример обработки инцидента до и после

До Demisto



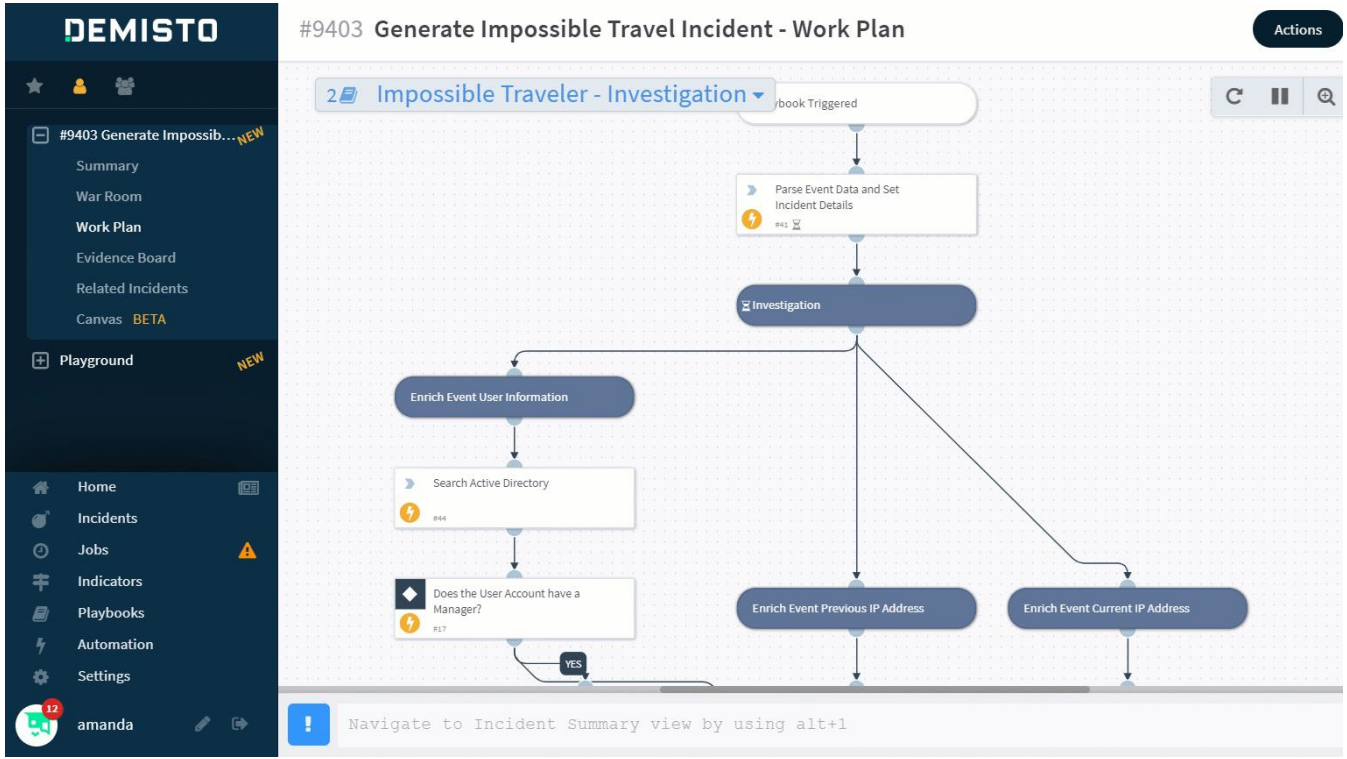
Disparate alert sources

Lack of defined process

Repetitive and manual actions

Lack of product interconnectivity

После внедрения XSOAR



Все события в одной консоли

Стандартизованные и реализованные процессы

Автоматизированные высоко частотные действия

Взаимодействие между продуктами

ИТОГИ

Итоги

- SOC – это не просто тренд, это центр оперативного реагирования для снижения рисков компрометации
- SOAR – система автоматизации, оркестрами и реагирования позволяющая повысить эффективность SOC в разы
- Cortex XSOAR - позволяет реализовать среду обработки инцидентов
- Cortex XSOAR – поддерживает из коробки интеграцию с 480+ системами и 1000+ автоматизаций
- Cortex XSOAR – это удобная платформа построения и стандартизации процессов/workflow/playbooks
- Cortex XSOAR – это платформа управления лентами Threat Intelligence (TIM)
- Cortex XSOAR – использует машинное обучение и платформу Docker

Дальнейшие Шаги

Рассмотренные решения

- NGFW – может применяться для решения специфических задач в OT и для решения большого комплекса задач в IT
- Cortex XDR – мощная платформа по блокированию угроз и идентификации продвинутых угроз на конечных рабочих станциях и в сетевом трафике с полной аналитикой и возможность реагирования
- (преимущественно для IT сетей и отдельных машин из OT-сетей)
- Cortex XSOAR – это среда автоматизации обработки инцидентов, позволяющая существенно снизить риски и увеличить эффективность SOC-ов (обработка OT и IT-инцидентов)

Дальнейшие шаги:

- Индивидуальная встреча по возможностям сегментации сети, дизайн с опором на ваши задачи (NGFW)
- Индивидуальная презентация и демонстрация Cortex XDR
- Индивидуальная презентация и демонстрация Cortex XSOAR

Специализированная

Thank you