Qualys.

mars solutions

Информационная безопасность для защиты вашей компании

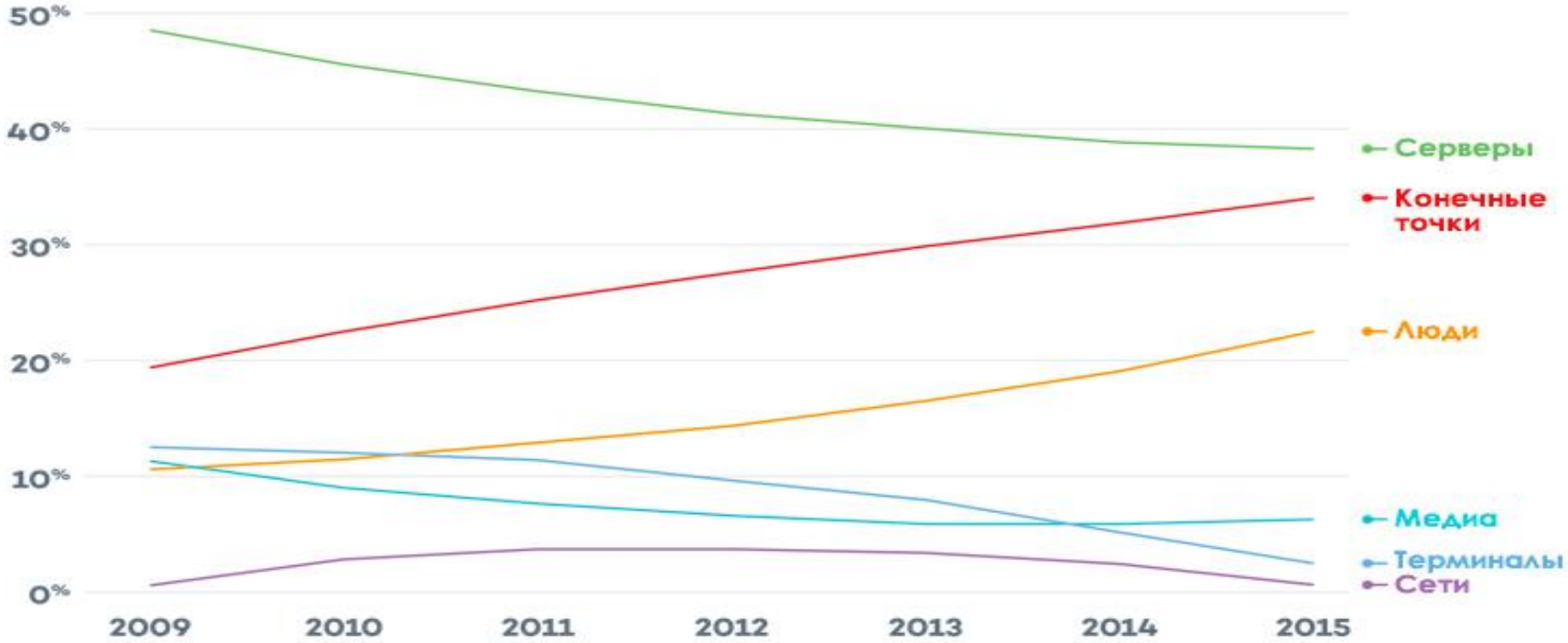
Pavel Kozlov
Project Manager, Mars Solutions

Тренды

- HBO
- KRACK
- Equifax
- WannaCry
- Petya/NotPetya
- Центральный банк Бангладеш, Philippines 2016

Qualys.

Цель злоумышленника – конечные устройства

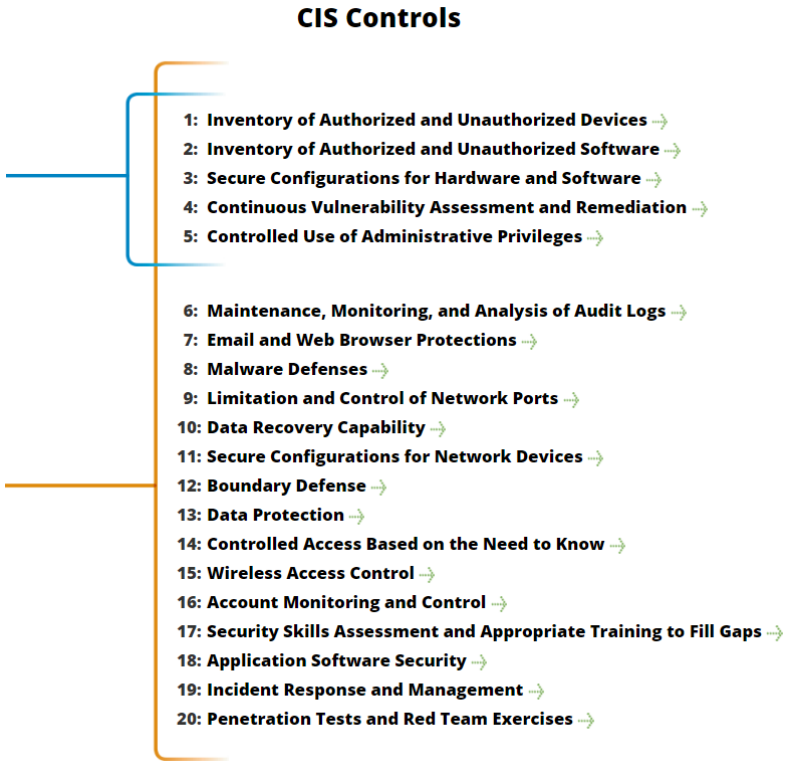


Qualys.

20 Критических контролей

Первые 5 контролей CIS

Все 20 контролей CIS



Qualys.

Первые 5 Критических Контролей

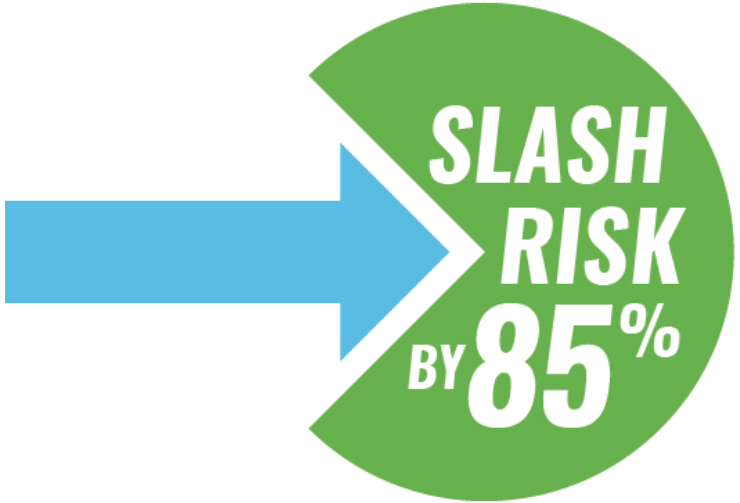
Реестр авторизованных и неавторизованных устройств

Реестр авторизованного и неавторизованного софта

Защищённые конфигурации для конечных устройств

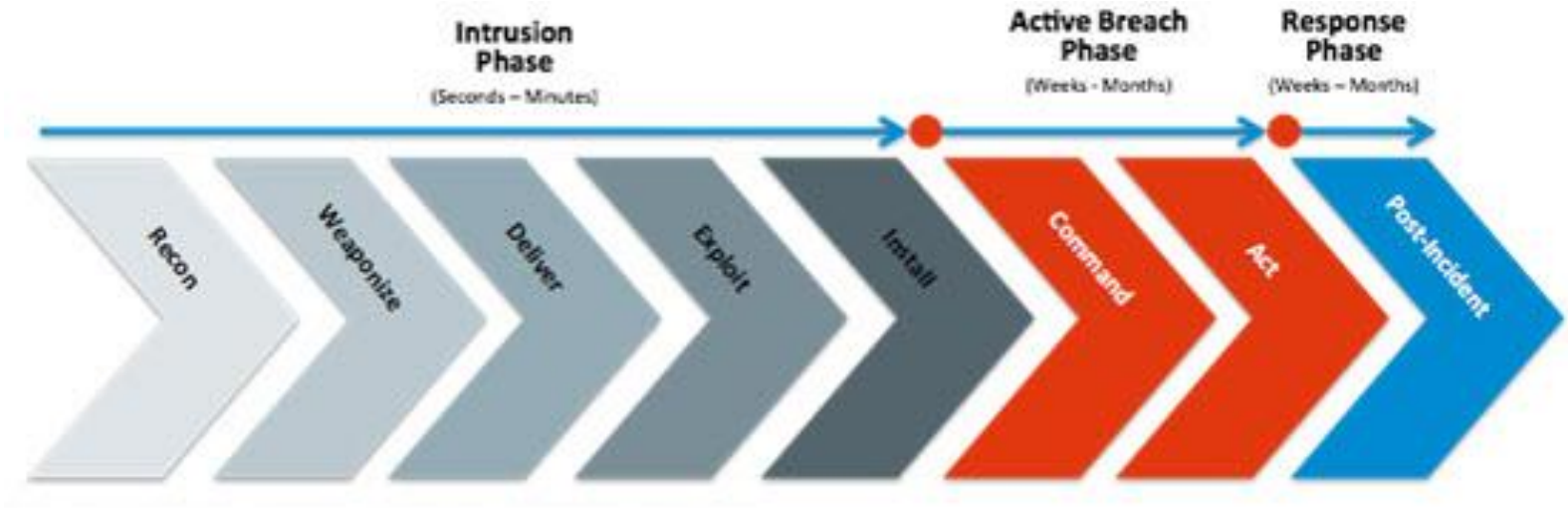
Непрерывный анализ защищённости и устранение проблем

Контролируемое использование административных привилегий



Qualys.

Cyber Kill Chain

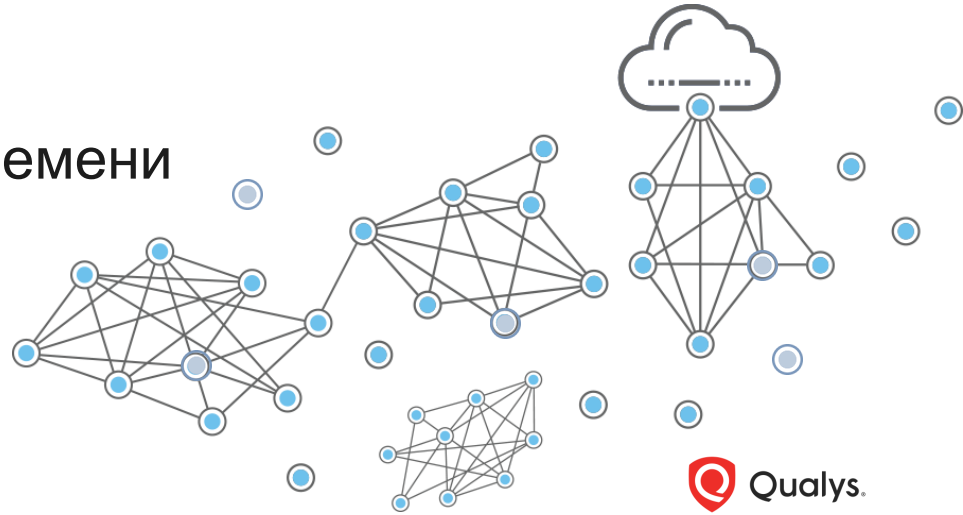


Qualys.

Полный контроль своей IT инфраструктуры

Надо знать о своих устройствах, где бы они не находились

В любой момент времени



Qualys.

Детальное понимание конфигураций

Информация по устройствам нужна для приоритезации и расследований

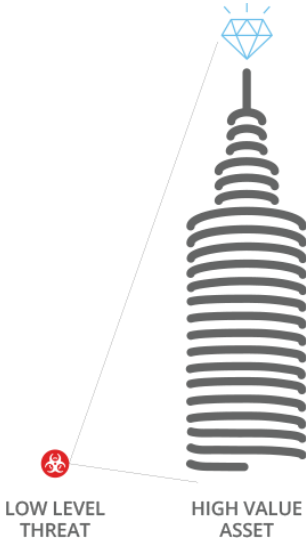
- Параметры железа
- Установленное ПО
- Запущенные сервисы
- Пользователи
- Установленные патчи
- **Уязвимости**
- Ошибки конфигураций

Qualys.

3 Оценка критичности устройств

Все устройства разные и имеют разные угрозы

- Внешние / Внутренние
- Рабочая станция / Сервер
- Критически важные данные
- Определённые параметры непрерывности работы



Qualys.

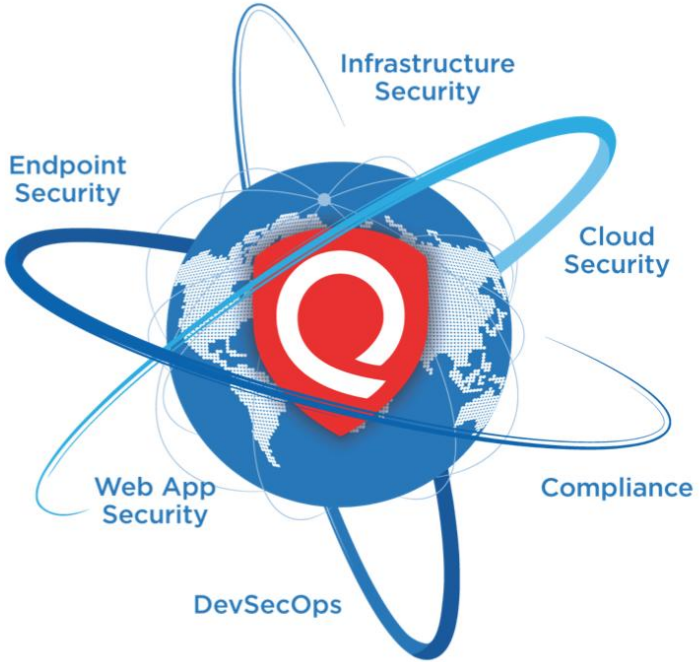
Возможность интерактивного поиска по проблемам и инцидентам

Правильная визуализация помогает повысить эффективность во много раз

- Виджеты/Дэшборды
- Оповещения
- Отчёты

Qualys.

Одна платформа для многих задач



Qualys.

Облачная платформа Qualys

Приложения Qualys

CA AI VM CM TP PC SAQ PCI WAS WAF

Qualys API

Аналитика и корреляция данных

- Reporting & Dashboards
- Remediation and Workflows
- Distributed Correlation
- ElasticSearch Clusters
- Solr Lucene Indexing
- Oracle and BFFS Storage

Распределённые сенсоры

Hardware Virtual Cloud Agent Passive API

3+ миллиарда
Сканирований в год

100 миллиардов
срабатываний

1+ триллион
Событий безопасности

Частное облако Qualys (PCPa)

Для хранения данных внутри компании

Поддерживает 30K VM/30K PC/3K WAS сканов в сутки

Управляется Qualys

Qualys.

Предотвратить инциденты

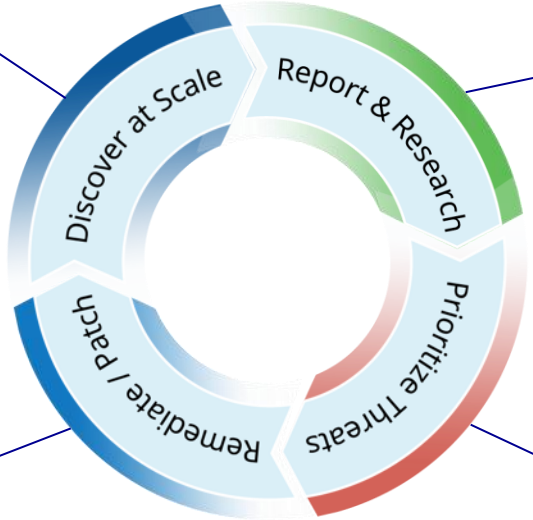
Vulnerability Management

Policy Compliance

Web Application Scanning

Continuous Monitoring

Asset Inventory



Patch Management*

WAF

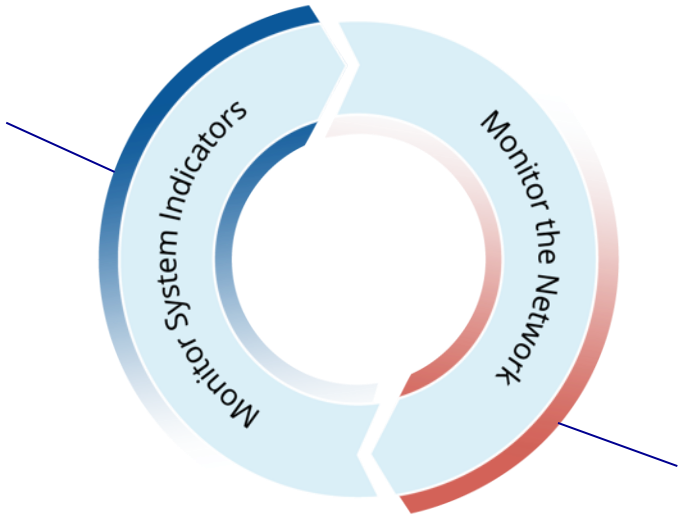
Threat Protection

Qualys.

Определить инциденты на ранних стадиях

Indication of Compromise

File Integrity Monitoring



Passive Network Analyzer*

Qualys.

Asset Inventory

Получите полную и мгновенную видимость Ваших ИТ активов

- Облачное решение для полного видения всех ваши ИТ активов, где бы они не находились

Asset Inventory

- Детальная информация о Вашем оборудовании
- Установленное ПО, версии ПО, включая приложения, ОС, драйверы, утилиты и т.д.
- Наличие уязвимостей и доступных обновлений
- Сервисы, файловые системы, запущенные процессы, ключи реестра

Vulnerability management and Continuous Monitoring

Непрерывное обнаружение изменений и защита от атак, везде и в любое время

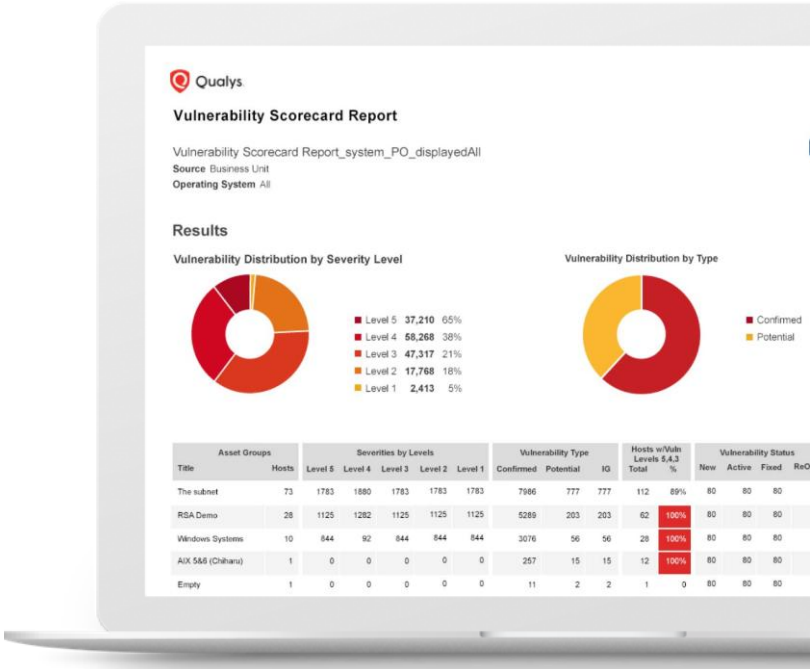
VM CM

Vulnerability management
and
Continuous Monitoring

Идентифицируйте и приоритезируйте угрозы

Vulnerability Management

- Приоритезируйте уязвимости согласно бизнес критичности
- Непрерывно следите за Вашим периметром на наличие неавторизованных изменений
- Отслеживайте уязвимости на протяжении всего времени: по мере появления, после исправления, в случае их повторного обнаружения
- Определите какие ОС, порты, сервисы и сертификаты используются оборудованием в вашей сети
- Проводите сканирование вашей сети в ручную, автоматически или непрерывно
- Сконцентрируйтесь на исправлении критически важных уязвимостей



Qualys.

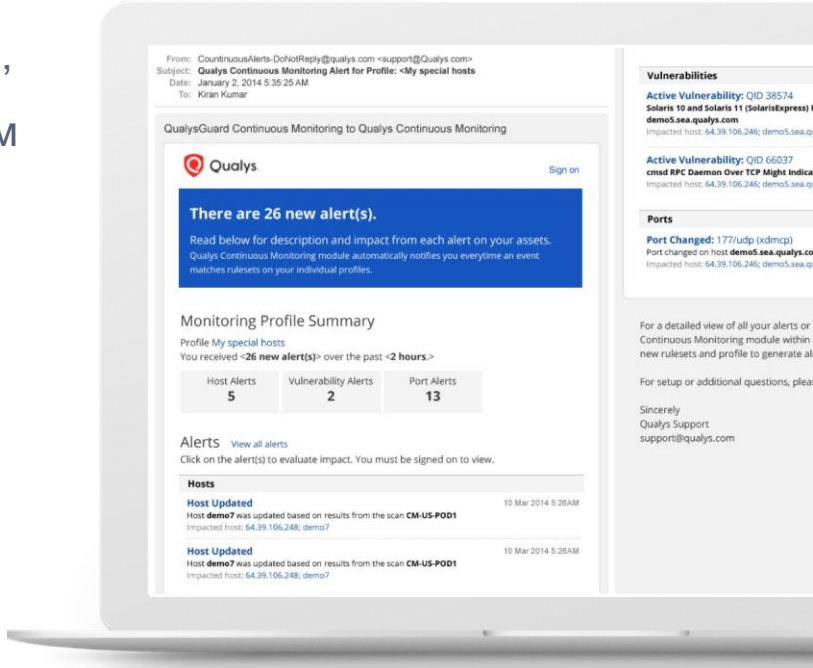
Улучшите и оптимизируйте Вашу сетевую безопасность

Continuous Monitoring

Непрерывно следя за изменениями в Вашей сети, до того как они привели к инциденту, CM даёт Вам полноценное и актуальное видение вашей ИТ инфраструктуры.

В том числе:

- Новое/Неавторизованное оборудование
- Порты: Небезопасные протоколы(telnet, ftp, Rlogin…etc)
- Уязвимости: DoS, remote code execution, PCI
- Нежелательно ПО: Уязвимые ПО/ОС



Qualys.

Cloud Agent для сканирования сети

Быстрое нахождение уязвимостей

Обнаруживайте и исправляйте уязвимости быстрее

Не нужны изменения на межсетевом экране

Поддержка оборудования, которое не может быть просканировано стандартными средствами

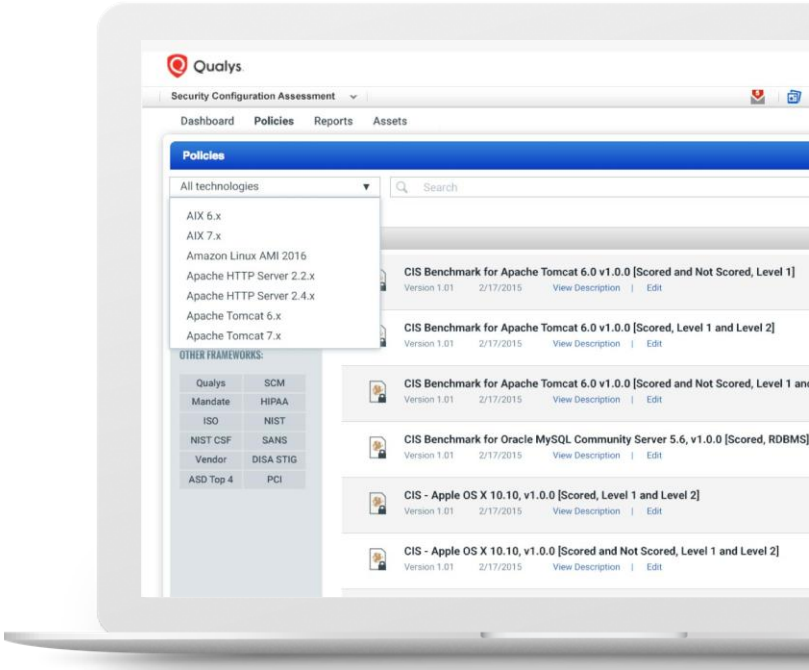
- Не возможно получить учётные записи для сканирования
- Удалённые устройства вне корпоративной сети
- Сервера чувствительные к сетевому сканированию

Qualys.

Qualys Security Configuration Assessment

Security Configuration Assessment

- Дополнение к VM
- Поддержка многих платформ
- Простая процедура оценки
- Удалённое сканирование через агент
- Использование лучших практик в своей работе

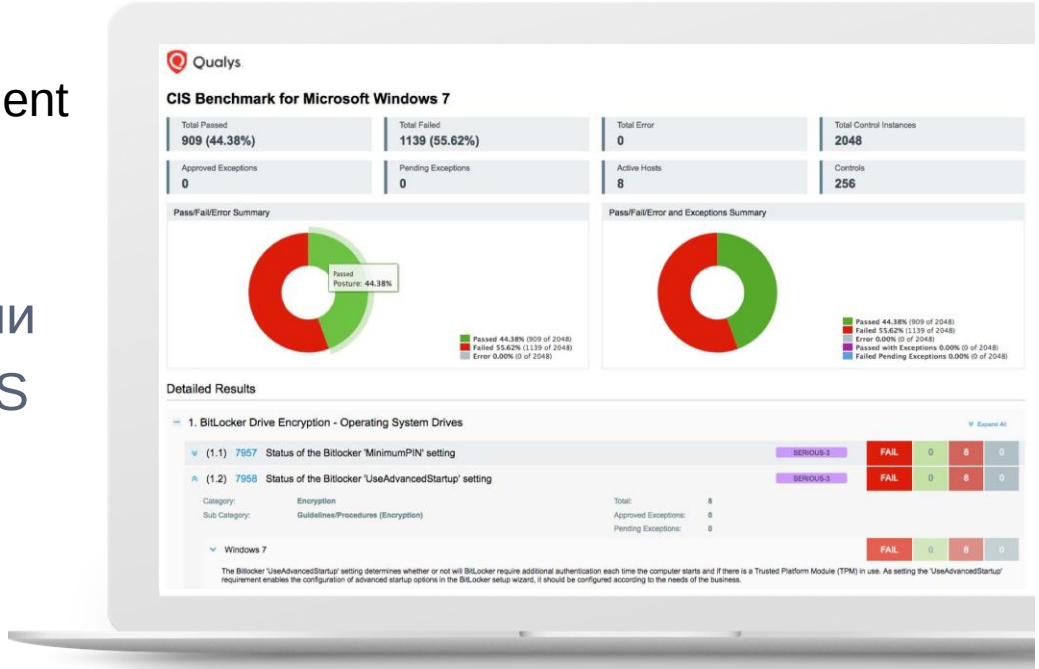


Qualys.

Security Configuration Assessment Process

Security Configuration Assessment

- Определить системы
- Собрать данные конфигурации
- Определить отклонения от CIS benchmark
- Создать удобный отчёт для дальнейшей работы



Qualys.

Indication of Compromise

Непрерывно следите и своевременно обнаруживайте подозрительную активность на ваших устройствах

- Облачное решение для маркировки данных, которые могут указывать на вредоносное ПО или нарушения на устройствах в сети и за ее пределами

Qualys.

Архитектура Qualys IOC

Qualys Malware Labs

Malware family models

Threat feeds

Threat feeds

OpenIOC files

SIEM via API

Splunk App

Qradar App

ServiceNow App

Offline search / hunt / investigate

CM Alerting

Visualize report pivot

FILE PROCESS REGISTRY NETWORK

Cloud Agent

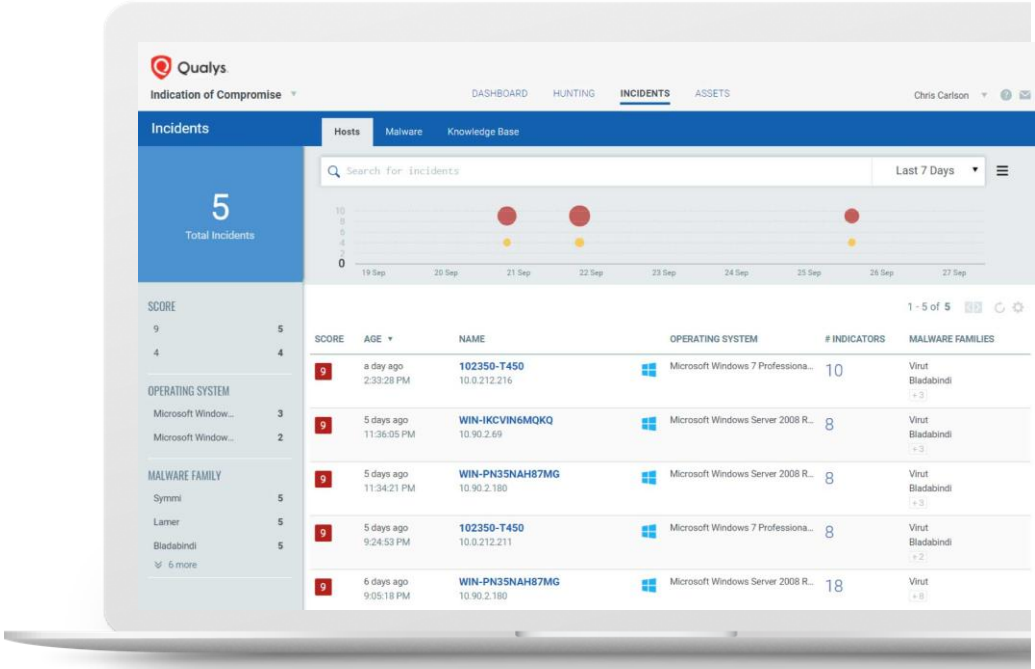
IOC

VM PC AI FIM

Qualys.

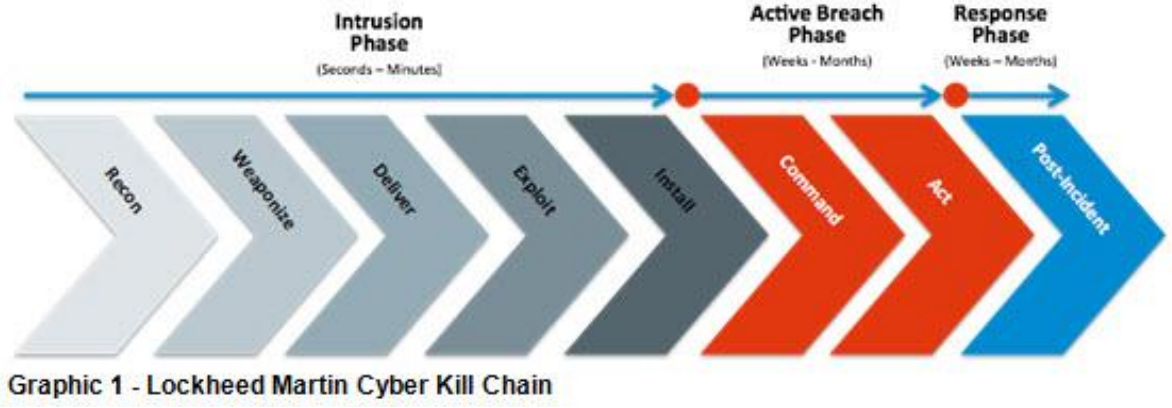
Indication of Compromise

- Автоматическое определение нового вредоносного ПО
- Улучшите безопасность конечных устройств благодаря обнаружению вредоносных программ, которые не находятся стандартными средствами.
- Быстрый и удобный поиск по индикаторам компрометации

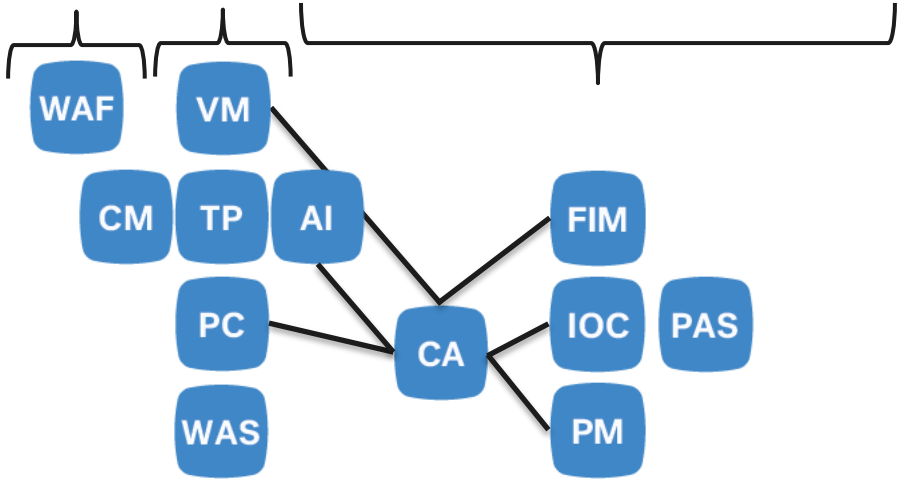


Qualys.

Cyber Kill Chain



Graphic 1 - Lockheed Martin Cyber Kill Chain



Qualys.

20 Critical Controls

- CSC 1: Inventory of Authorized and Unauthorized Devices
- CSC 2: Inventory of Authorized and Unauthorized Software
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges
- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 7: Email and Web Browser Protections
- CSC 8: Malware Defenses
- CSC 9: Limitation and Control of Network Ports, Protocols, and Services
- CSC 10: Data Recovery Capability
- CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- CSC 12: Boundary Defense
- CSC 13: Data Protection
- CSC 14: Controlled Access Based on the Need to Know
- CSC 15: Wireless Access Control
- CSC 16: Account Monitoring and Control
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 18: Application Software Security
- CSC 19: Incident Response and Management
- CSC 20: Penetration Tests and Red Team Exercises

Qualys.

Blue Chip Global Customer Base

70% of the Forbes Global 100 and
25% of the Forbes Global 2,000

- 9 of the top 10 in Major Banks
- 9 of the top 10 in Software
- 8 of the top 10 in Consumer Discretionary
- 8 of the top 10 in Consumer Staples
- 8 of the top 10 in Technology
- 7 of top 10 in Telecommunications
- 6 of top 10 in Healthcare
- 5 of top 10 in Energy & Utilities
- 5 of top 10 in Industrial & Materials
- 5 of top 10 in Insurance

Qualys.

Резюмируя

- Если вы действительно хотите защитить свою сеть, то вы должны знать свою сеть.

- Qualys поможет Вам:
  - Обеспечить контроль **всей** Вашей инфраструктуры
  - Максимально быстро узнавать о проблемах и инцидентах
  - Обнаружить и приоритизировать наиболее уязвимы места
  - Снизить затраты на обслуживание систем
  - Повысить эффективность IT отдела

- Что можно сделать прямо сейчас:
  - Получите **бесплатное демо на 30 дней** на вашу инфраструктуру

Qualys.

mars solutions

Спасибо!

Email: pavel.kozlov@followmars.com
Mobile phone: +998 93 171 05 53