CISCO
SECURE

Как построить ИБ в большой компании?

Пошаговый план

Алексей Лукацкий

Бизнес-консультант по безопасности

alukatsk@cisco.com

CISCO The bridge to possible

Плановая или навязанная цифровая трансформация

То, что было задумано давно и реально нужно (или навязано) бизнесу

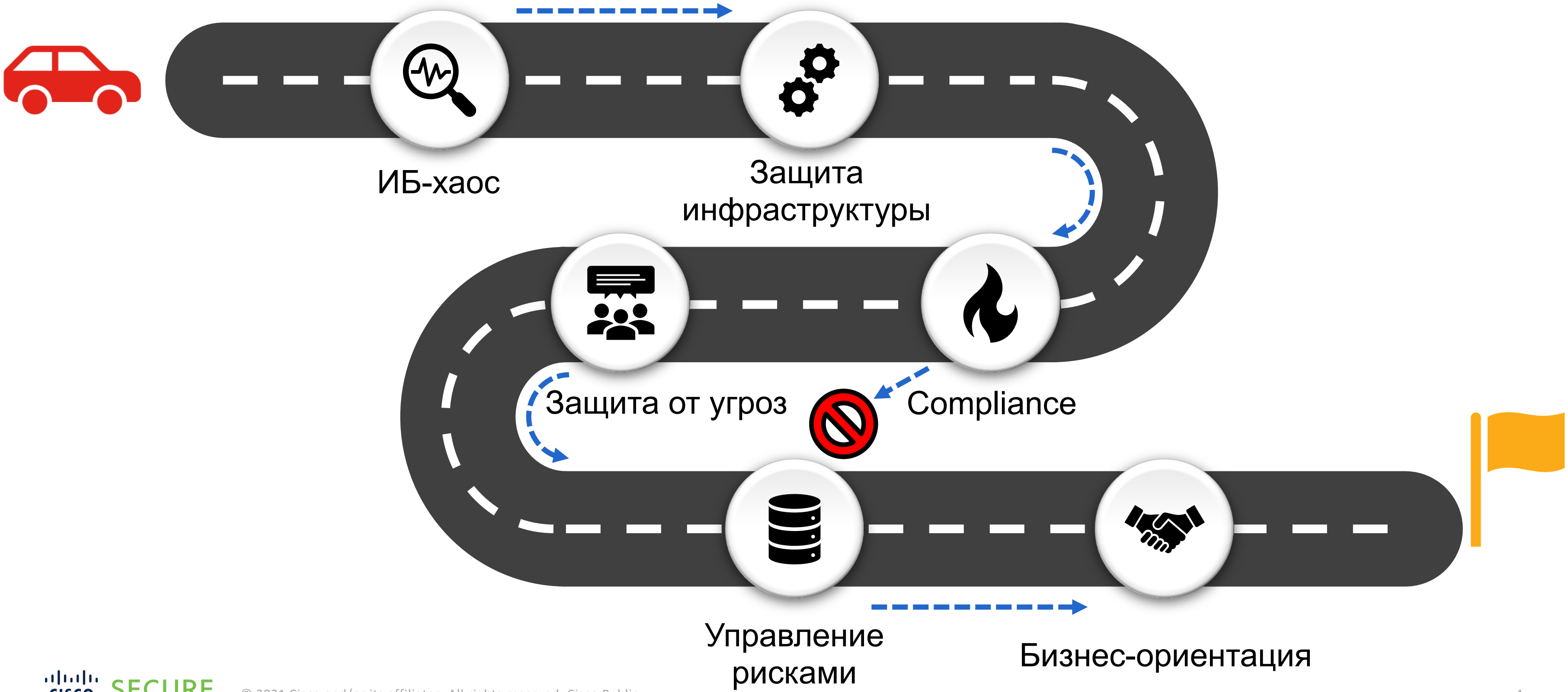
- Цифровые платформы
- Цифровые двойники
- Роботизация
- Искусственный интеллект
- Большие данные
- Блокчейн
- Офис будущего

Авральная цифровизация

То, что нужно бизнесу, но возникло внезапно и неожиданно

- Удаленный доступ
- Удаленное обслуживание клиентов
- Средства групповой работы
- Электронный документооборот
- Торговые Интернет-площадки

Каждая компания имеет свой уровень зрелости ИБ



Но если бы у нас был green field?

4 популярных стратегии построения ИБ

С точки зрения активов

Классический ИТшник

Защищаем то, что есть в инфраструктуре – ЦОДы, облака, унифицированные коммуникации, Wi-Fi, ERP, OT/ICS и т.п.

С точки зрения угроз

Начинающий ИБшник

Защищаем не «ЧТО», а «ОТ ЧЕГО», даже если эти угрозы никак не влияют бизнес или ИТ

С точки зрения требований регуляторов

Проженный силовик

Законодательство создано для того, чтобы его соблюдать. Бизнес и ИТ должны выполнять все требования регуляторов

С точки зрения защитных мер

Продвинутый ИБшник

Современные защитные меры позволяют нейтрализовать все угрозы, защитить современные ИТ и даже выполнить требования регуляторов (наверное)

Нормативное регулирование ИБ в банках

НПС
- 382-П
- 683-П
- 672-П
- Антифрод

Персданные
- ФЗ-152
- Приказ ФСТЭК №21
- Приказ ФСБ №378
- Приказы РКН

ЕБС / УИК
- ФЗ-115
- 4859-У
- 4-МР
- Приказы Минцифры

Опер.риски
- Резервирование капитала
- Проект Положения БР

PCI DSS
- PCI DSS
- PA DSS
- HSM

Критическая инфра.
- ФЗ-187
- ПП-127
- Приказы ФСТЭК
- Приказы ФСБ

Финтех
- Цифровой профиль
- СБП
- Open API
- Маркетплейс

СПФС
- Письмо ЦБ №04-45/2470

GDPR
- GDPR

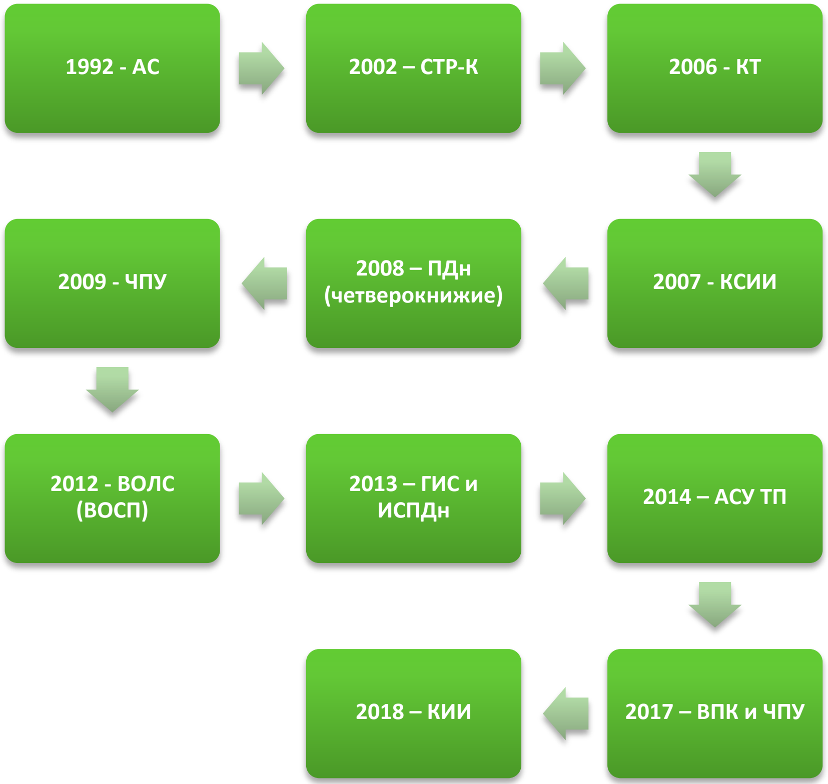
Криптография
- Приказы ФСБ
- ФЗ-63 (по электронной подписи)

SWIFT
- CSP SCF

ГОСТы
- 57580.1
- 57580.2
- Еще 15 проектов

Только один пример - ФСТЭК

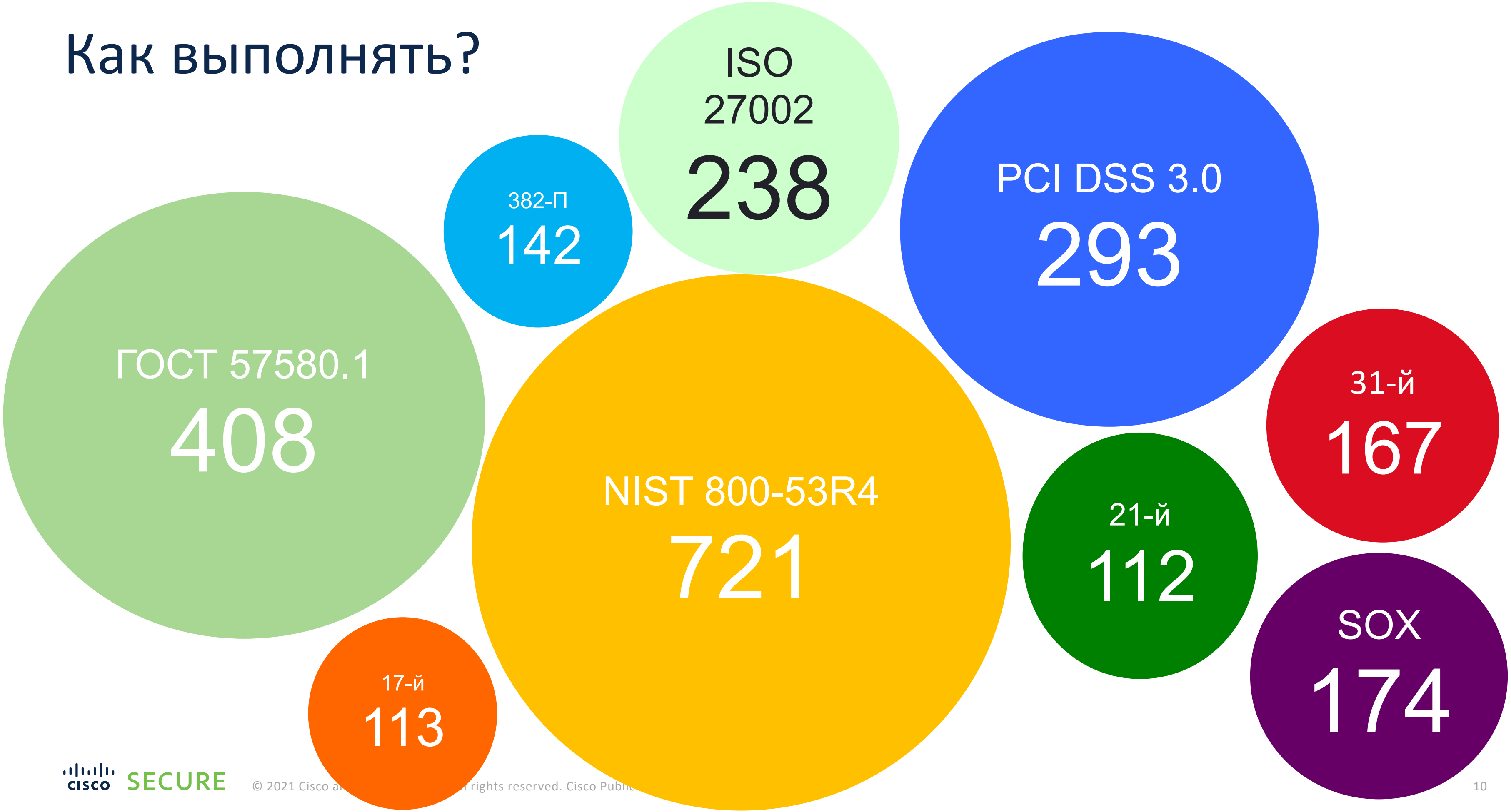
Большое количество требований не позволяет реализовать их последовательно. Особенно в контексте появления новых требований и вовлечения новых регуляторов



Что надо сделать для обеспечения безопасности?

- Назначение ответственных
- Моделирование угроз
- Выработка защитных мер
- Разработка организационно-распорядительной и эксплуатационной документации
- Выбор, приобретение, внедрение и эксплуатация защитных средств
- Управление ИБ
- Реагирование на инциденты
- Анализ уязвимостей
- Мониторинг ИБ

Как выполнять?



«Небольшая доля причин, вкладываемых средств или прилагаемых усилий, отвечает за большую долю результатов, получаемой продукции или заработанного вознаграждения»

Вильфредо Парето (1848 – 1923)

10 базовых защитных мер

С чего стоило бы начать реализацию защитных мер по требованиям ФСТЭК

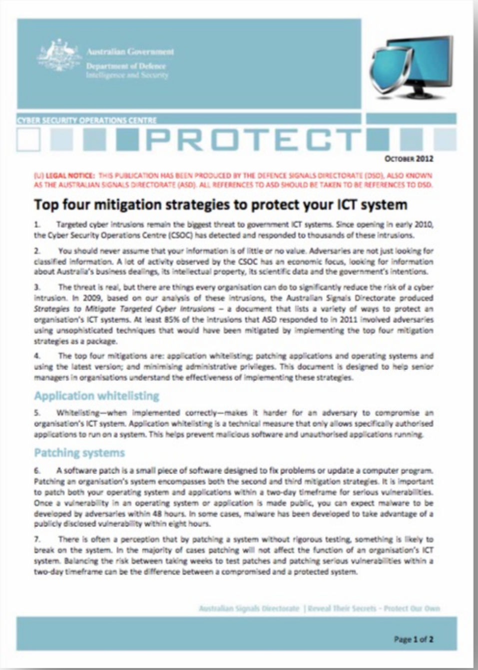
- **ОПС.3** - Установка (инсталляция) только разрешенного к использованию ПО и (или) его компонентов
- **АНЗ.2** - Контроль установки обновлений ПО, включая обновление ПО средств защиты информации
- **АНЗ.3** - Контроль работоспособности, параметров настройки и правильности функционирования ПО и средств защиты информации
- **АНЗ.5** - Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация прав разграничения доступа, полномочий пользователей в информационной системе
- **УПД.5** - Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы

10 базовых защитных мер

С чего стоило бы начать реализацию защитных мер по требованиям ФСТЭК

- **ИАФ.1** - Идентификация и аутентификация пользователей, являющихся работниками оператора
- **ИАФ.2** - Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
- **ОДТ.4** - Периодическое резервное копирование информации на резервные машинные носители информации
- **ОДТ.2** - Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы
- **ЗИС.17** - Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы.

Топ 4 защитных мер (по версии австралийского регулятора)



Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

October 2012

(U) LEGAL NOTICE: THIS PUBLICATION HAS BEEN PRODUCED BY THE DEFENCE SIGNALS DIRECTORATE (DSD), ALSO KNOWN AS THE AUSTRALIAN SIGNALS DIRECTORATE (ASD). ALL REFERENCES TO ASD SHOULD BE TAKEN TO BE REFERENCES TO DSD.

Top four mitigation strategies to protect your ICT system

1. Targeted cyber intrusions remain the biggest threat to government ICT systems. Since opening in early 2010, the Cyber Security Operations Centre (CSOC) has detected and responded to thousands of these intrusions.

2. You should never assume that your information is of little or no value. Adversaries are not just looking for classified information. A lot of activity observed by the CSOC has an economic focus, looking for information about Australia's business dealings, its intellectual property, its scientific data and the government's intentions.

3. The threat is real, but there are things every organisation can do to significantly reduce the risk of a cyber intrusion. In 2009, based on our analysis of these intrusions, the Australian Signals Directorate produced *Strategies to Mitigate Targeted Cyber Intrusions* – a document that lists a variety of ways to protect an organisation's ICT systems. At least 85% of the intrusions that ASD responded to in 2011 involved adversaries using unsophisticated techniques that would have been mitigated by implementing the top four mitigation strategies as a package.

4. The top four mitigations are: application whitelisting; patching applications and operating systems and using the latest version; and minimising administrative privileges. This document is designed to help senior managers in organisations understand the effectiveness of implementing these strategies.

Application whitelisting

5. Whitelisting—when implemented correctly—makes it harder for an adversary to compromise an organisation's ICT system. Application whitelisting is a technical measure that only allows specifically authorised applications to run on a system. This helps prevent malicious software and unauthorised applications running.

Patching systems

6. A software patch is a small piece of software designed to fix problems or update a computer program. Patching an organisation's system encompasses both the second and third mitigation strategies. It is important to patch both your operating system and applications within a two-day timeframe for serious vulnerabilities. Once a vulnerability in an operating system or application is made public, you can expect malware to be developed by adversaries within 48 hours. In some cases, malware has been developed to take advantage of a publicly disclosed vulnerability within eight hours.

7. There is often a perception that by patching a system without rigorous testing, something is likely to break on the system. In the majority of cases patching will not affect the function of an organisation's ICT system. Balancing the risk between taking weeks to test patches and patching serious vulnerabilities within a two-day timeframe can be the difference between a compromised and a protected system.

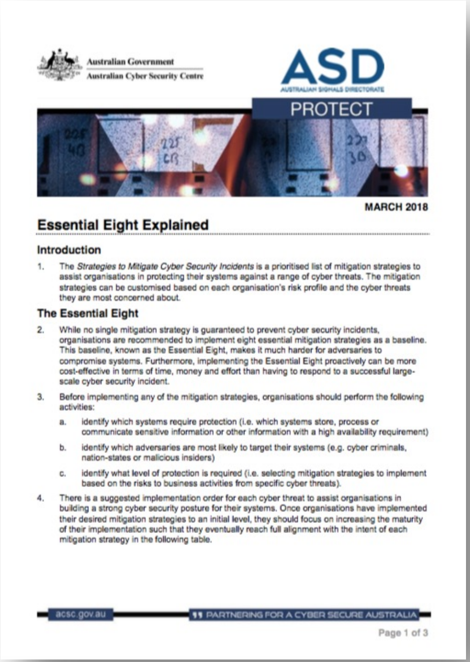
Australian Signals Directorate | Reveal Their Secrets – Protect Our Own

Page 1 of 2

1. Application whitelisting (замкнутая программная среда)
2. Обновление приложений (установка патчей)
3. Обновление операционных систем
4. Ограничение административных привилегий

Закрывают 85% всех угроз

Топ 8 защитных мер (по версии австралийского регулятора)


Australian Government
Australian Cyber Security Centre

ASD
AUSTRALIAN SIGNALS DIRECTORATE
PROTECT

MARCH 2018

Essential Eight Explained

Introduction

1. The *Strategies to Mitigate Cyber Security Incidents* is a prioritised list of mitigation strategies to assist organisations in protecting their systems against a range of cyber threats. The mitigation strategies can be customised based on each organisation's risk profile and the cyber threats they are most concerned about.

The Essential Eight

2. While no single mitigation strategy is guaranteed to prevent cyber security incidents, organisations are recommended to implement eight essential mitigation strategies as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems. Furthermore, implementing the Essential Eight proactively can be more cost-effective in terms of time, money and effort than having to respond to a successful large-scale cyber security incident.
3. Before implementing any of the mitigation strategies, organisations should perform the following activities:
   a. identify which systems require protection (i.e. which systems store, process or communicate sensitive information or other information with a high availability requirement)
   b. identify which adversaries are most likely to target their systems (e.g. cyber criminals, nation-states or malicious insiders)
   c. identify what level of protection is required (i.e. selecting mitigation strategies to implement based on the risks to business activities from specific cyber threats).
4. There is a suggested implementation order for each cyber threat to assist organisations in building a strong cyber security posture for their systems. Once organisations have implemented their desired mitigation strategies to an initial level, they should focus on increasing the maturity of their implementation such that they eventually reach full alignment with the intent of each mitigation strategy in the following table.

acsc.gov.au
PARTNERING FOR A CYBER SECURE AUSTRALIA
Page 1 of 3

1. Application whitelisting (замкнутая программная среда)
2. Обновление приложений (установка патчей)
3. Конфигурация настроек макросов в MS Office
4. Усиление защиты приложений пользователей (отключение Flash, блокирование Java и скриптов и т.п.)
5. Ограничение административных привилегий
6. Многофакторная аутентификация
7. Обновление операционных систем
8. Ежедневное резервное копирование

Закрывают 90% всех угроз

Топ 37 защитных мер (по версии австралийского регулятора)

Mitigation Strategy Effectiveness Ranking for 2014 (and 2012)	Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Helps Detect Intrusions	Helps Prevent Intrusion Stage 1: Code Execution	Helps Contain Intrusion Stage 2: Network Propagation	Helps Contain Intrusion Stage 3: Data Exfiltration
1 (1)	**Application whitelisting** of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.	Essential	Medium	High	Medium	Yes	Yes	Yes	Yes
2 (2)	**Patch applications** e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.	Essential	Low	High	High	No	Yes	Possible	No
3 (3)	**Patch operating system vulnerabilities.** Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.	Essential	Low	Medium	Medium	No	Yes	Possible	No
4 (4)	**Restrict administrative privileges** to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.	Essential	Medium	Medium	Low	No	Possible	Yes	No

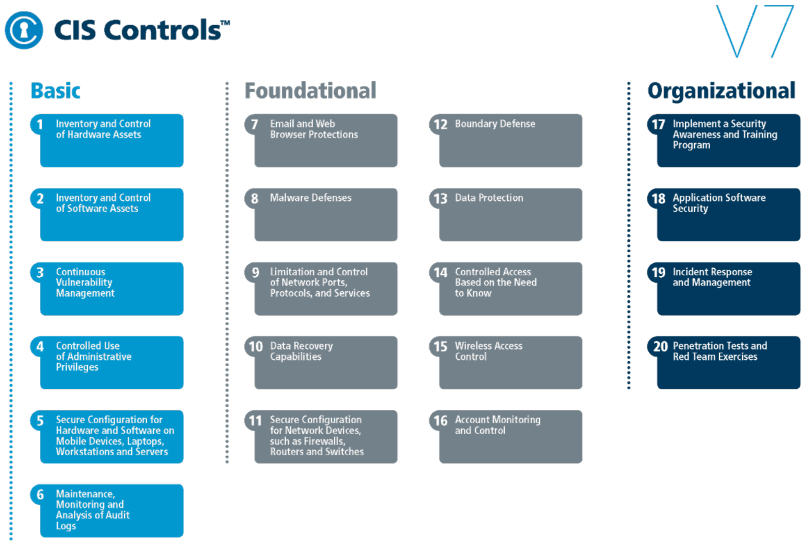
Once organisations have effectively implemented the Top 4 mitigation strategies, firstly on workstations of users who are most likely to be targeted by cyber intrusions and then on all workstations and servers, additional mitigation strategies can then be selected to address security gaps until an acceptable level of residual risk is reached.

Mitigation Strategy Effectiveness Ranking for 2014 (and 2012)	Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Helps Detect Intrusions	Helps Prevent Intrusion Stage 1: Code Execution	Helps Contain Intrusion Stage 2: Network Propagation	Helps Contain Intrusion Stage 3: Data Exfiltration
5 (18)	**User application configuration hardening,** disabling: running Internet-based Java code, untrusted Microsoft Office macros, and unneeded/undesired web browser and PDF viewer features.	Excellent	Medium	Medium	Medium	No	Yes	No	No
6 (N/A)	**Automated dynamic analysis** of email and web content run in a sandbox to detect suspicious behaviour including network traffic, new or modified files, or other configuration changes.	Excellent	Low	Medium	Low	Yes	Yes	No	Possible
7 (21)	**Operating system generic exploit mitigation** e.g. Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).	Excellent	Low	Medium	Low	Possible	Yes	Possible	No
8 (11)	**Host-based Intrusion Detection/Prevention System** to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence.	Excellent	Low	Medium	Medium	Yes	Yes	No	Possible
9 (5)	**Disable local administrator accounts** to prevent network propagation using compromised local administrator credentials that are shared by several workstations.	Excellent	Low	Medium	Low	No	No	Yes	No
10 (7)	**Network segmentation and segregation** into security zones to protect sensitive information and critical services such as user authentication by the Microsoft Active Directory service.	Excellent	Low	High	Medium	Yes	No	Yes	Possible
11 (6)	**Multi-factor authentication** especially implemented for remote access, or when the user is about to perform a privileged action or access a sensitive information repository.	Excellent	Medium	High	Medium	No	No	Possible	No
12 (8)	**Software-based application firewall, blocking incoming network traffic** that is malicious or otherwise unauthorised, and denying network traffic by default.	Excellent	Low	Medium	Medium	Yes	Yes	Yes	No
13 (9)	**Software-based application firewall, blocking outgoing network traffic** that is not generated by a whitelisted application, and denying network traffic by default.	Excellent	Medium	Medium	Medium	Yes	No	Yes	Yes
14 (10)	**Non-persistent virtualised sandboxed trusted operating environment,** hosted outside of the organisation's internal network, for risky activities such as web browsing.	Excellent	High	High	Medium	Possible	No	Yes	Possible
15 (12)	**Centralised and time-synchronised logging of successful and failed computer events,** with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low	High	High	Yes	No	Possible	Possible
16 (13)	**Centralised and time-synchronised logging of allowed and blocked network activity,** with automated immediate log analysis, storing logs for at least 18 months.	Excellent	Low	High	High	Yes	No	Possible	Possible
17 (14)	**Email content filtering,** allowing only whitelisted business related attachment types. Preferably analyse/convert/sanitise hyperlinks, PDF and Microsoft Office attachments.	Excellent	High	High	Medium	Yes	Yes	No	Possible
18 (15)	**Web content filtering** of incoming and outgoing traffic, whitelisting allowed types of web content and using behavioural analysis, cloud-based reputation ratings, heuristics and signatures.	Excellent	Medium	Medium	Medium	Yes	Yes	No	Possible
19 (16)	**Web domain whitelisting for all domains,** since this approach is more proactive and thorough than blacklisting a tiny percentage of malicious domains.	Excellent	High	High	Medium	Yes	Yes	No	Yes
20 (19)	**Block spoofed emails** using Sender ID or Sender Policy Framework (SPF) to check incoming emails, and a "hard fail" SPF record to help prevent spoofing of your organisation's domain.	Excellent	Low	Low	Low	Possible	Yes	No	No
21 (22)	**Workstation and server configuration management** based on a hardened Standard Operating Environment, disabling unneeded/undesired functionality e.g. IPv6, autorun and LanMan.	Good	Medium	Medium	Low	Possible	Yes	Yes	Possible
22 (25)	**Antivirus software using heuristics and automated Internet-based reputation ratings** to check a program's prevalence and its digital signature's trustworthiness prior to execution.	Good	Low	Low	Low	Yes	Yes	No	No
23 (24)	**Deny direct Internet access from workstations** by using an IPv6-capable firewall to force traffic through a split DNS server, an email server, or an authenticated web proxy server.	Good	Low	Low	Low	Yes	Possible	No	Yes
24 (23)	**Server application configuration hardening** e.g. databases, web applications, customer relationship management, finance, human resources and other data storage systems.	Good	Low	High	Medium	Possible	Yes	No	Possible
25 (27)	**Enforce a strong passphrase policy** covering complexity, length, expiry, and avoiding both passphrase reuse and the use of a single dictionary word.	Good	Medium	Medium	Low	Possible	No	Yes	No
26 (29)	**Removable and portable media control** as part of a Data Loss Prevention strategy, including storage, handling, whitelisting allowed USB devices, encryption and destruction.	Good	High	Medium	Medium	No	Yes	Possible	Yes
27 (28)	**Restrict access to Server Message Block (SMB) and NetBIOS** services running on workstations and on servers where possible.	Good	Low	Medium	Low	No	Yes	Yes	No
28 (20)	**User education** e.g. Internet threats and spear phishing socially engineered emails. Avoid: weak passphrases, passphrase reuse, exposing email addresses, unapproved USB devices.	Good	Medium	High	Medium	Possible	Possible	No	No
29 (26)	**Workstation inspection of Microsoft Office files** for potentially malicious abnormalities e.g. using the Microsoft Office File Validation or Protected View feature.	Good	Low	Low	Low	Possible	Yes	No	No
30 (25)	**Signature-based antivirus software** that primarily relies on up to date signatures to identify malware. Use gateway and desktop antivirus software from different vendors.	Good	Low	Low	Low	Possible	Possible	No	No
31 (30)	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and used for social engineering. Perform content scanning after email traffic is decrypted.	Good	Low	Low	Low	No	No	No	No
32 (32)	**Block attempts to access websites by their IP address** instead of by their domain name, e.g. implemented using a web proxy server, to force cyber adversaries to obtain a domain name.	Average	Low	Low	Low	Yes	Yes	No	Yes
33 (33)	**Network-based Intrusion Detection/Prevention System** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Average	Low	High	High	Possible	Possible	Possible	Possible
34 (34)	**Gateway blacklisting** to block access to known malicious domains and IP addresses, including dynamic and other domains provided free to anonymous Internet users.	Average	Low	Low	High	Possible	Yes	No	Yes
35 (35)	**Capture network traffic** to/from internal critical asset workstations and servers as well as traffic traversing the network perimeter, to perform post-intrusion analysis.	Average	Low	High	Low	No	No	No	No

- Essential
- Excellent
- Very Good
- Good
- Limited

Топ20 CIS Controls

- Схожая идеология
- Начиналось как проект SANS Top20
- 20 блоков защитных мер
- Базовый и фундаментальный уровни + оргмеры



В мае будет анонсирована версия 8

Топ20 CIS Controls

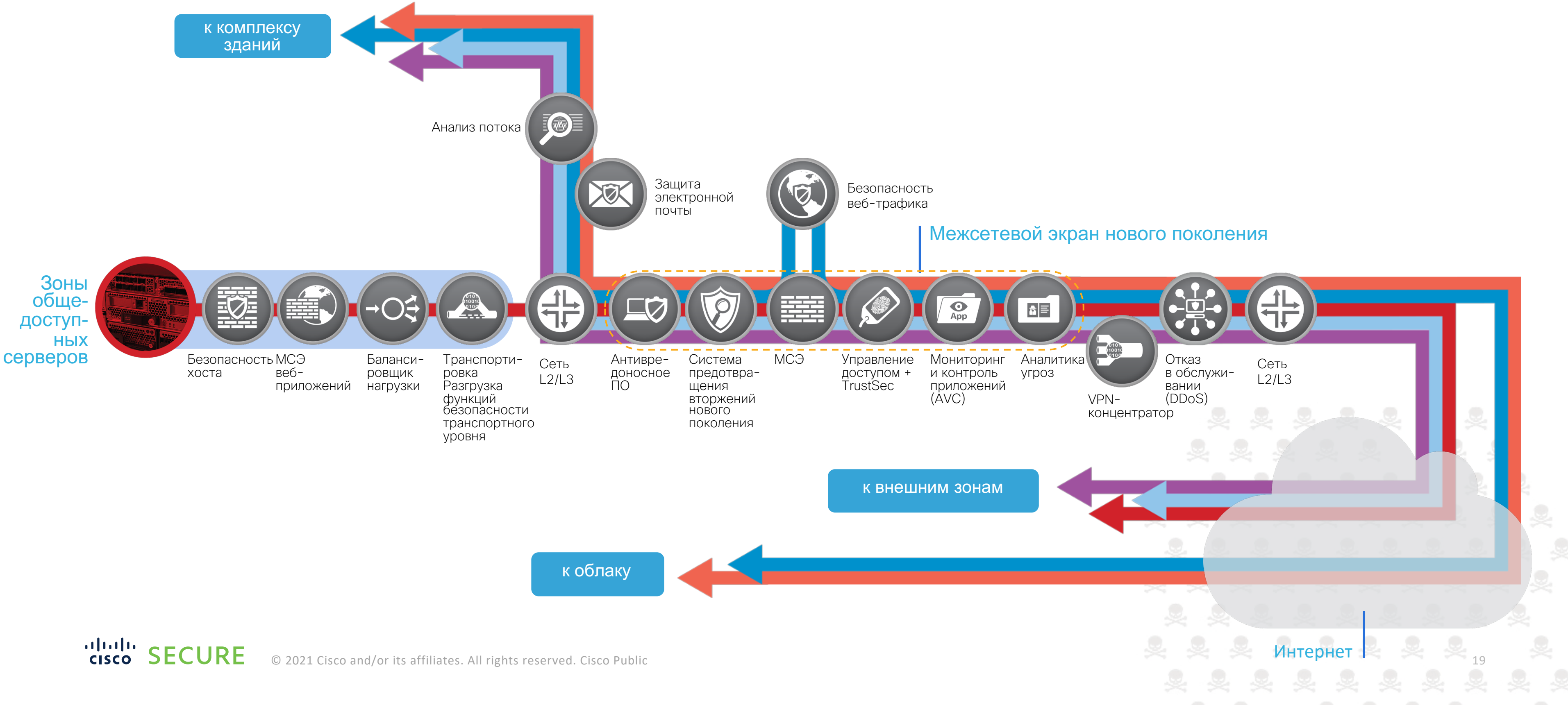
- Все меры объединены в группы реализации (implementation group)
- Учет компаний разного размера, с разными ресурсами, разной экспертизой в ИБ, разной зрелостью и моделью угроз

17-20 Organizational

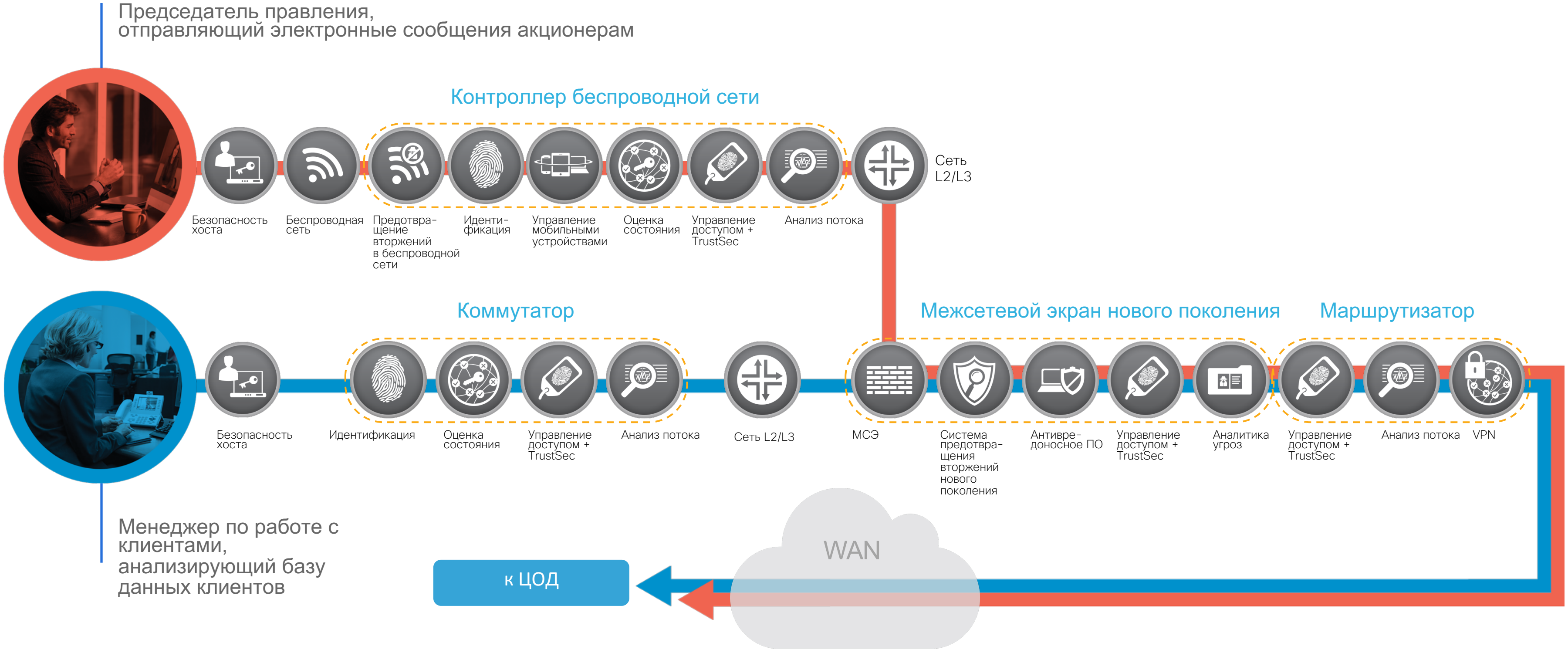
CIS Sub-Control	CIS Control Title	Implementation Groups 1	2	3
CIS Control 16:	**Account Monitoring and Control**			
16.1	Maintain an Inventory of Authentication Systems		●	●
16.2	Configure Centralized Point of Authentication		●	●
16.3	Require Multi-Factor Authentication		●	●
16.4	Encrypt or Hash All Authentication Credentials		●	●
16.5	Encrypt Transmittal of Username and Authentication Credentials		●	●
16.6	Maintain an Inventory of Accounts		●	●
16.7	Establish Process for Revoking Access		●	●
16.8	Disable Any Unassociated Accounts	●	●	●
16.9	Disable Dormant Accounts	●	●	●
16.10	Ensure All Accounts Have An Expiration Date		●	●
16.11	Lock Workstation Sessions After Inactivity	●	●	●
16.12	Monitor Attempts to Access Deactivated Accounts		●	●
16.13	Alert on Account Login Behavior Deviation			●
CIS Control 17:	**Implement a Security Awareness and Training Program**			
17.1	Perform a Skills Gap Analysis		●	●
17.2	Deliver Training to Fill the Skills Gap		●	●
17.3	Implement a Security Awareness Program	●	●	●
17.4	Update Awareness Content Frequently		●	●
17.5	Train Workforce on Secure Authentication	●	●	●
17.6	Train Workforce on Identifying Social Engineering Attacks	●	●	●
17.7	Train Workforce on Sensitive Data Handling	●	●	●
17.8	Train Workforce on Causes of Unintentional Data Exposure	●	●	●
17.9	Train Workforce Members on Identifying and Reporting Incidents	●	●	●

CIS Sub-Control	CIS Control Title	Implementation Groups 1	2	3
CIS Control 19:	**Incident Response and Management**			
19.1	Document Incident Response Procedures	●	●	●
19.2	Assign Job Titles and Duties for Incident Response		●	●
19.3	Designate Management Personnel to Support Incident Handling	●	●	●
19.4	Devise Organization-wide Standards For Reporting Incidents		●	●
19.5	Maintain Contact Information For Reporting Security Incidents	●	●	●
19.6	Publish Information Regarding Reporting Computer Anomalies and Incidents	●	●	●
19.7	Conduct Periodic Incident Scenario Sessions for Personnel		●	●
19.8	Create Incident Scoring and Prioritization Schema			●
CIS Control 20:	**Penetration Tests and Red Team Exercises**			
20.1	Establish a Penetration Testing Program		●	●
20.2	Conduct Regular External and Internal Penetration Tests		●	●
20.3	Perform Periodic Red Team Exercises			●
20.4	Include Tests for Presence of Unprotected System Information and Artifacts		●	●
20.5	Create a Test Bed for Elements Not Typically Tested in Production		●	●
20.6	Use Vulnerability Scanning and Penetration Testing Tools in Concert		●	●
20.7	Ensure Results From Penetration Test Are Documented Using Open, Machine-Readable Standards			●
20.8	Control and Monitor Accounts Associated With Penetration Testing		●	●

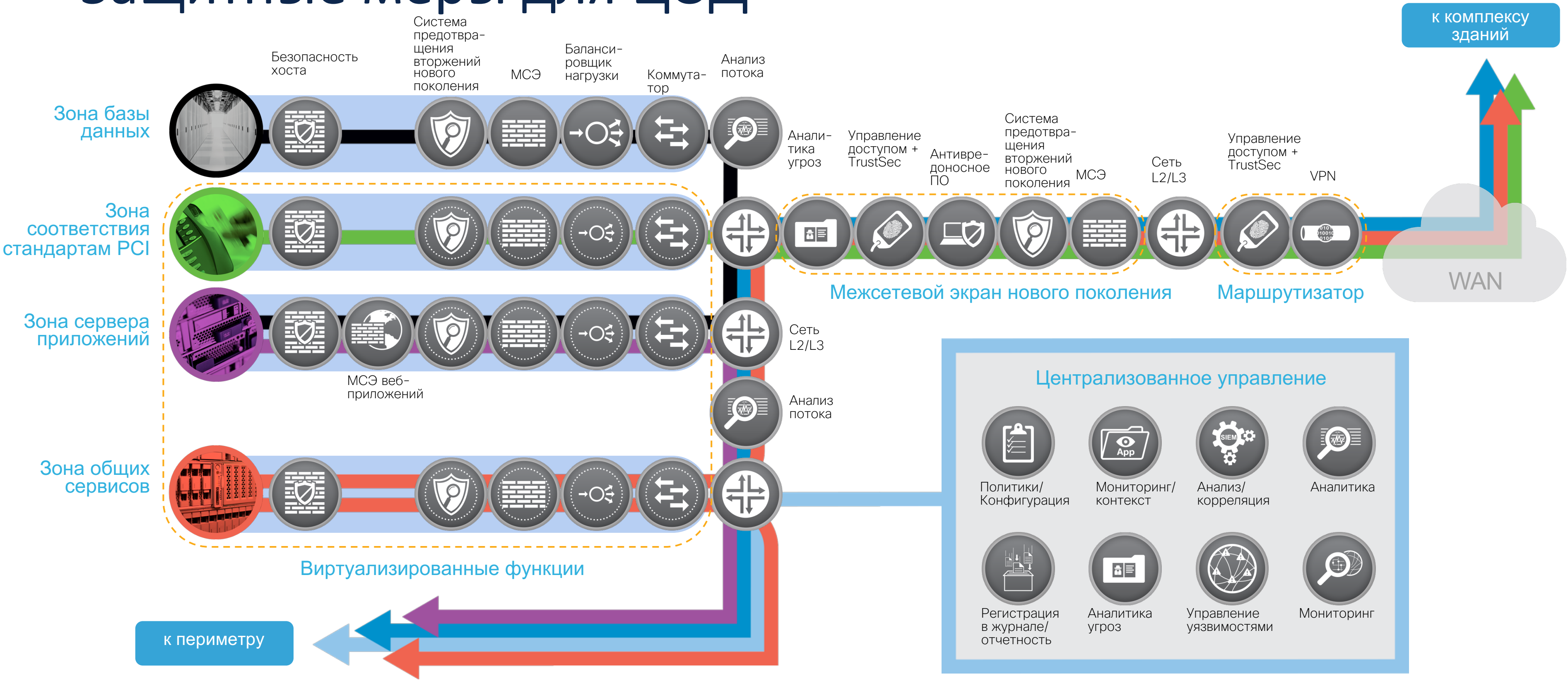
Защитные меры для периметра



Защитные меры для локальной сети



Защитные меры для ЦОД



CIS Benchmarks

Более 100 руководств по защите современных технологий от современных угроз

- Alibaba Cloud
- Amazon Web Services
- Apple MacOS
- CentOS
- Cisco
- Docker
- Google Cloud Platform
- IBM AIX
- Kubernetes
- MS Azure
- MS Office
- MongoDB
- NGINX
- Oracle DBMS / Linux
- Принтеры
- VMware
- Zoom

Как из кирпичиков собрать здание?

Начинается все с архитектуры ИБ

- Архитектура описывает желаемую структуру инфраструктуры безопасности организации и других связанных с ИБ компонентов и интерфейсов
  - Включает процессы, людей, технологии и разные типы информации
  - Создается с точки зрения бизнеса и учитывает его текущие и будущие потребности

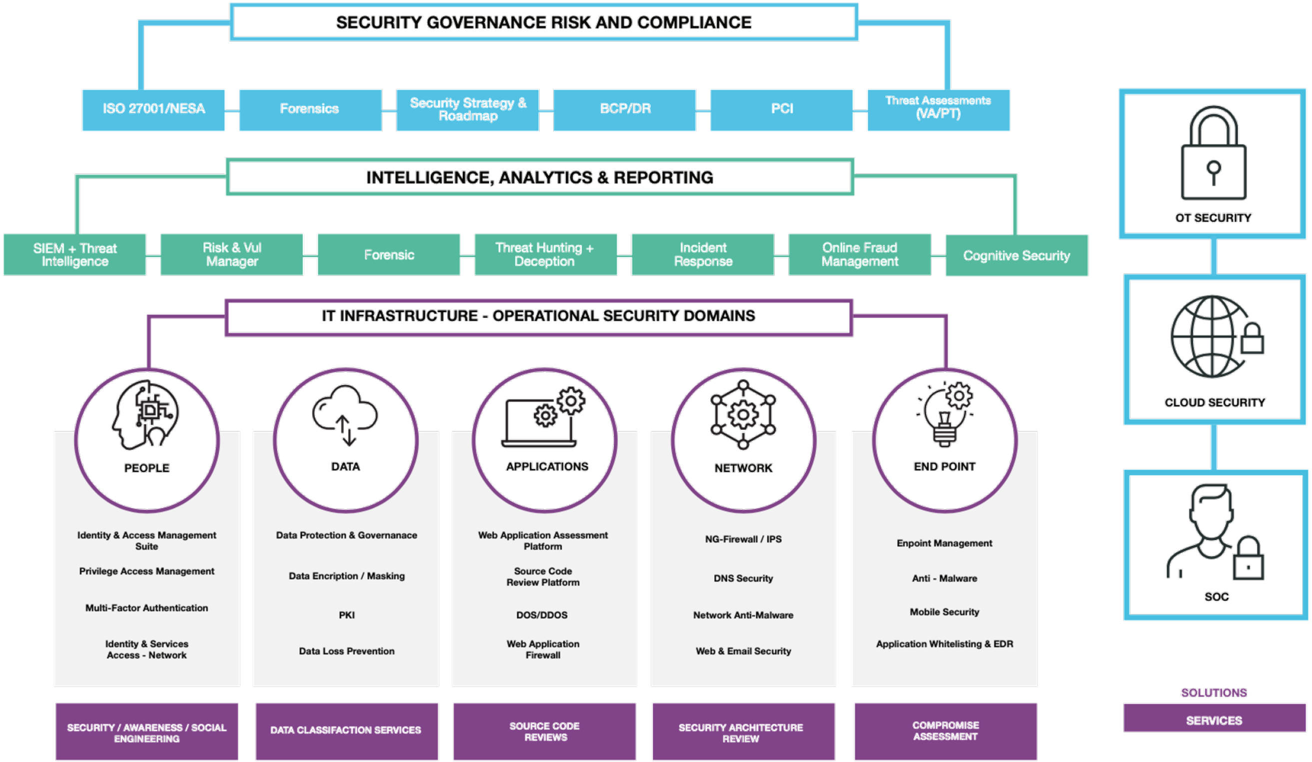
Архитектура ИБ

- Какие цели?
- Что требуется для достижения целей?

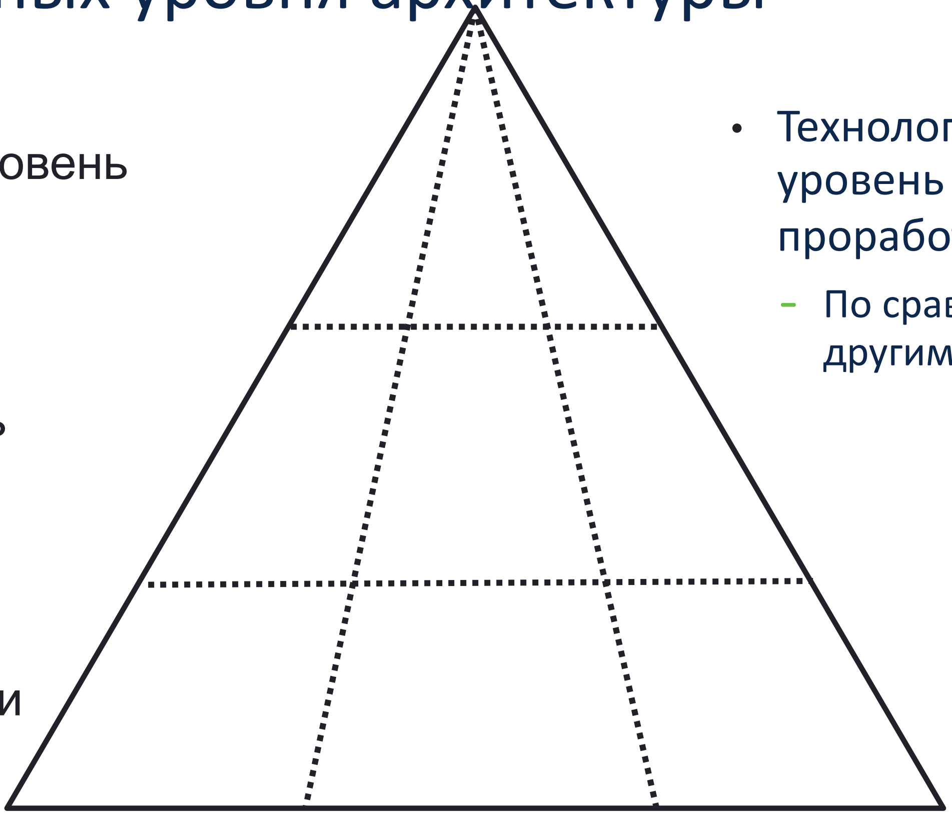
Стратегия ИБ

- Как могут быть достигнуты цели?

Пример: целевой архитектуры ИБ



3 горизонтальных уровня архитектуры



- Технологический уровень обычно проработан лучше всех
  - По сравнению с 2-мя другими уровнями

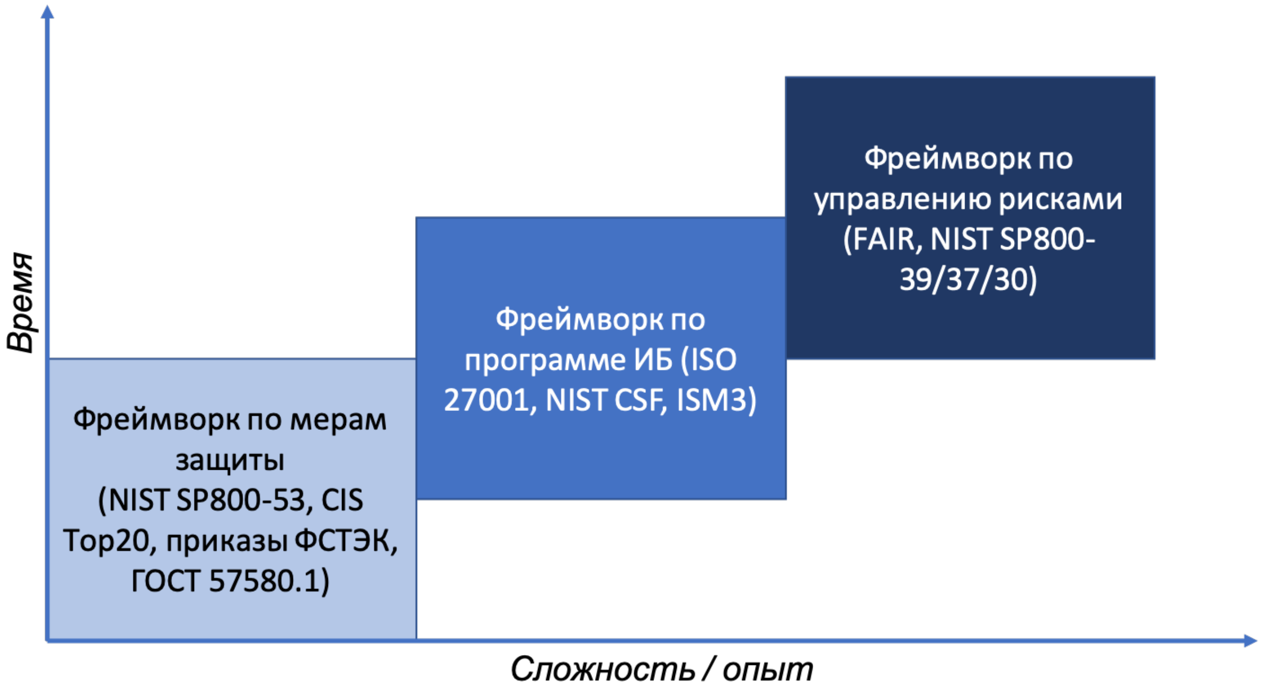
21 элемент стратегического, логического и технологического уровней архитектуры ИБ

Уровни доверия	Сервисы безопасности	Архитектура безопасности приложений
Концептуальные дизайны и модели	Модель доменов доверия	Архитектура сетевой/ инфраструктурной безопасности
Система взглядов на политики безопасности	Принципы дизайна защищенной инфраструктуры	Архитектура сервисов безопасности
Система взглядов на классификацию информации	Модели дизайна	Классификатор защищаемой информации
Процессная модель	Модель информационных потоков	Архитектура управления безопасности
Модель стратегических ролей и ответственности	Организационные модели	Принципы стандартизации и унификации ИБ
Миссия ИБ	Шаблоны требований	Организационная архитектура

Что такое фреймворк по ИБ?

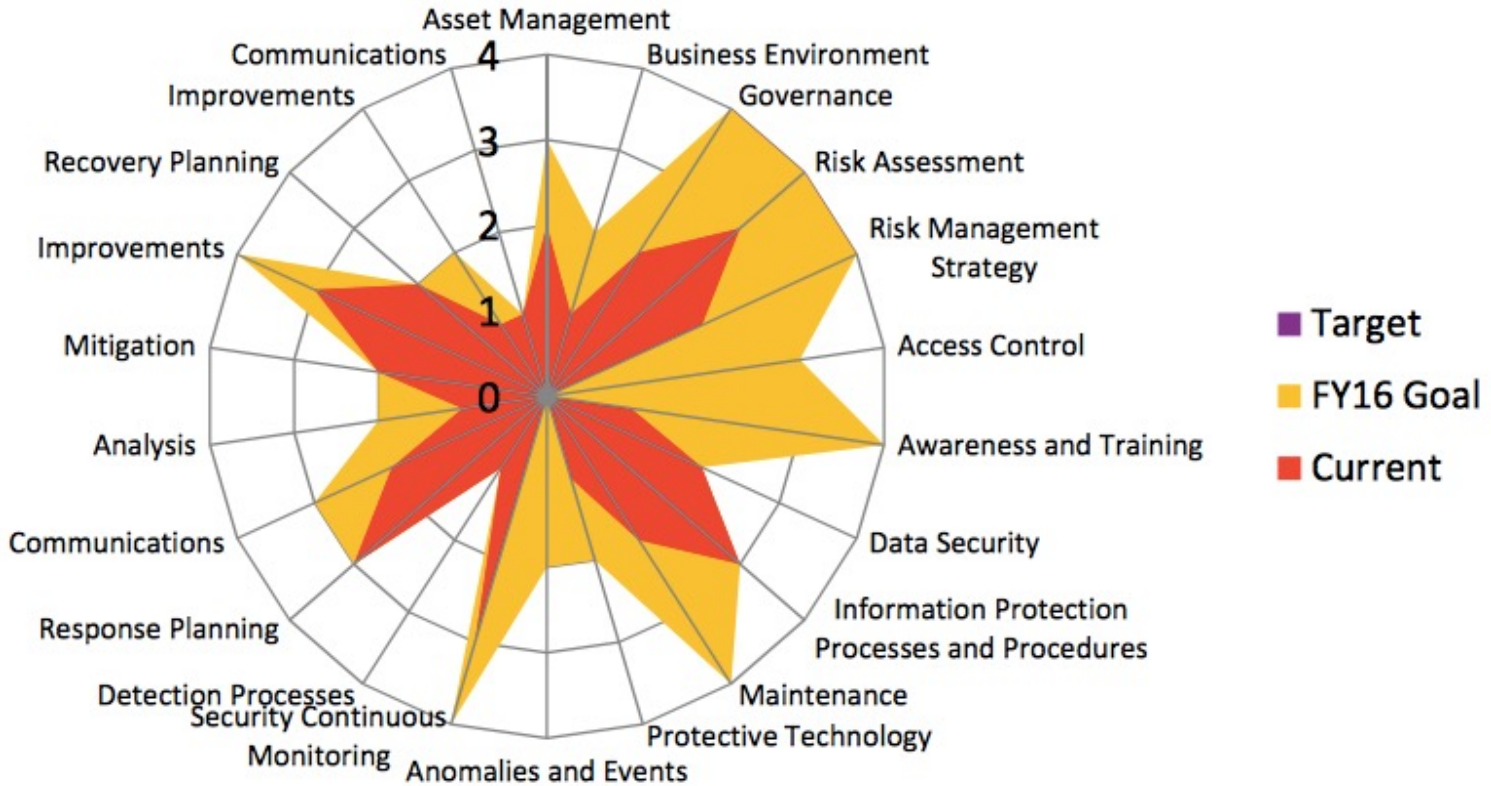
- Определение базового и расширенного набора защитных мер, подходящих конкретной организации
- Профилирование организаций исходя из разных требований и окружения
- Реализация набора защитных мер исходя из требований
- Оценка текущего состояния уровня защиты информации
- Приоритезации защитных мероприятий и составления дорожной карты развития

Фреймворки по ИБ: какие и для чего?



+ фреймворки по приватности, киберфизическим системам, персоналу и т.п.

Оценка зрелости ИБ по фреймворку



Какова цель вашей компании?

Рост прибыли / выручки / маржинальности / доли рынка?

You make security **possible**

Ответьте на 4 вопроса

- Что остановит или замедлит операции в вашей организации?
- Что приведет к снижению прибыли / выручки / маржинальности / доли рынка вашей компании?
- Что приведет к снижению качества предоставляемого вами продукта / услуги?
- Что приведет к негативному влиянию на цель компании / бизнес-подразделения / бизнес-проекта / executive sponsor?

cisco SECURE