Трансформация.
Успешная. Цифровая. Защищенная.

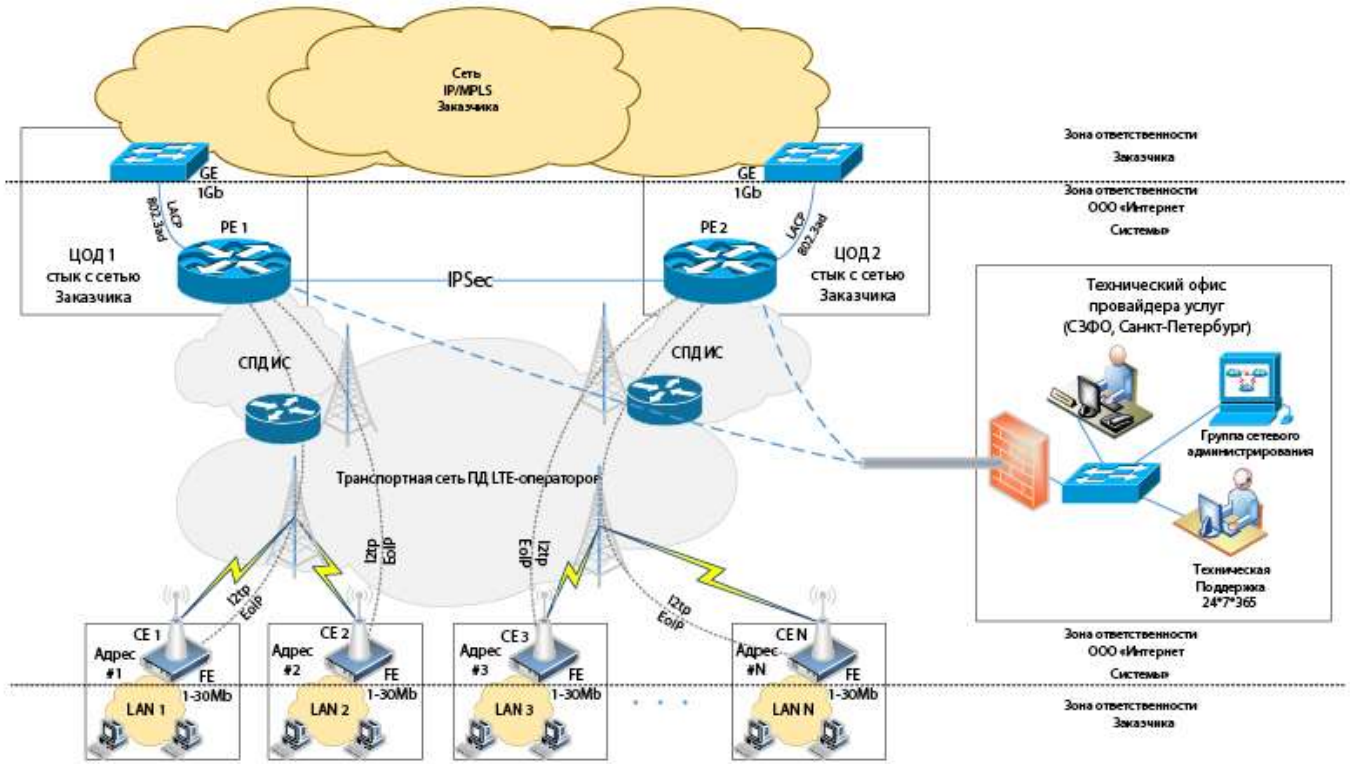
Архитектура безопасности

на скорую руку

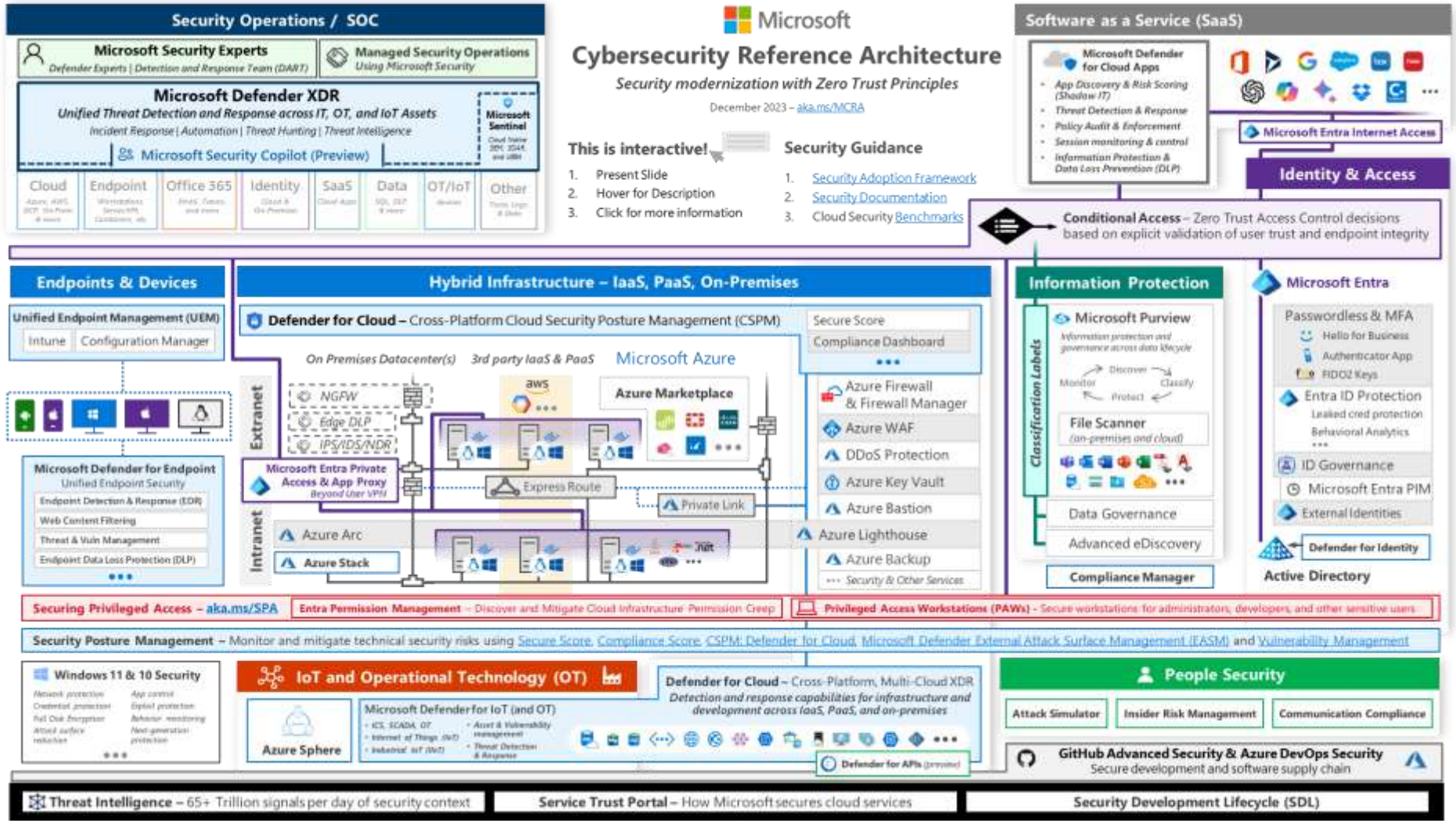
INFOSECURITY
a Softline company

Архитектура безопасности – это что?

Это просто схема сети



Это просто карточки для «бинго»



Это больше похоже. Но много букв.

Table 3-3: The 36-Cell SABSA® Matrix

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organisation and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Modes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management Support	Security of Sites, networks and Platforms	Security Operations Schedule

Учат в школе


Обследование
Формирование требований
Проектирование
Внедрение
Функционирование и поддержка

Комплаенс вечен

- Запаздывает
- Не специфичен либо слишком специфичен
- Слабо учитывает профиль рисков
- Создает ограничения для архитектуры
- Цель – соответствие требованиям (ни больше, ни меньше)

Слишком мало ресурсов и слишком много ресурсов – это почти одно и то же

- «Болезни роста» - это не только про бизнес.
  Бизнес тянет за собой ИТ, ИТ - тянет кибербез.
- Слишком много ресурсов не бывает. Не бывает же, правда?

- Все сойдется в одной точке, где нужно будет
  - отбросить неважное и несрочное
  - определить приоритеты среди важного
  - выбрать между «идеально, но никогда»
    и «на скорую руку, но сейчас»

Многовато для аксиом, когда идёт дым

Business Risk-Driven Security	Context	Scope	Intelligence	Trust	Holistic Approach
Simplicity	Reuse	Resilience	Process-Driven	Optimal Conflict Resolution	Communication Clarity
Usability	Security by Design	Precedence	Device Sovereignty	Defense in Depth	Least Privilege
		Manage Access	Communication Security		

(c) The Open Group Guide Axioms for the Practice of Security Architecture

Мой выбор, когда уже горит

Business Risk-Driven Security	Context	Scope	Intelligence	Trust	Holistic Approach
Simplicity	Reuse	Resilience	Process-Driven	Optimal Conflict Resolution	Communication Clarity
Usability	Security by Design	Precedence	Device Sovereignty	Defense in Depth	Least Privilege
		Manage Access	Communication Security		

ИТ-ландшафт как черный ящик

- Инвентаризация ИТ-активов – не то, чем кажется
- «Реверс-инжиниринг» сложившихся паттернов в ИТ важнее скурпулезного документирования архитектуры конкретных приложений
- Покрытие СЗИ - это про деньги. Важно понять то, что важно.

End-to-End во всём.
От требований - к юз-кейсам.

A.6.2 Мобильные устройства и дистанционная работа Цель: обеспечить безопасность при дистанционной работе и использовании мобильных устройств	
A.6.2.1	Следует определить политику и реализовать поддерживающие меры безопасности для управления рисками информационной безопасности, связанными с использованием мобильных устройств
A.6.2.2	Следует определить политику и реализовать поддерживающие меры безопасности для защиты информации, доступ к которой, обработка или хранение осуществляются в местах дистанционной работы

vs

Топ-менеджер компании приносит в офис личный MacBook и подключается к беспроводной сети для работы с электронной почтой и СЭДО.

Вопросы, которые нужно решить:

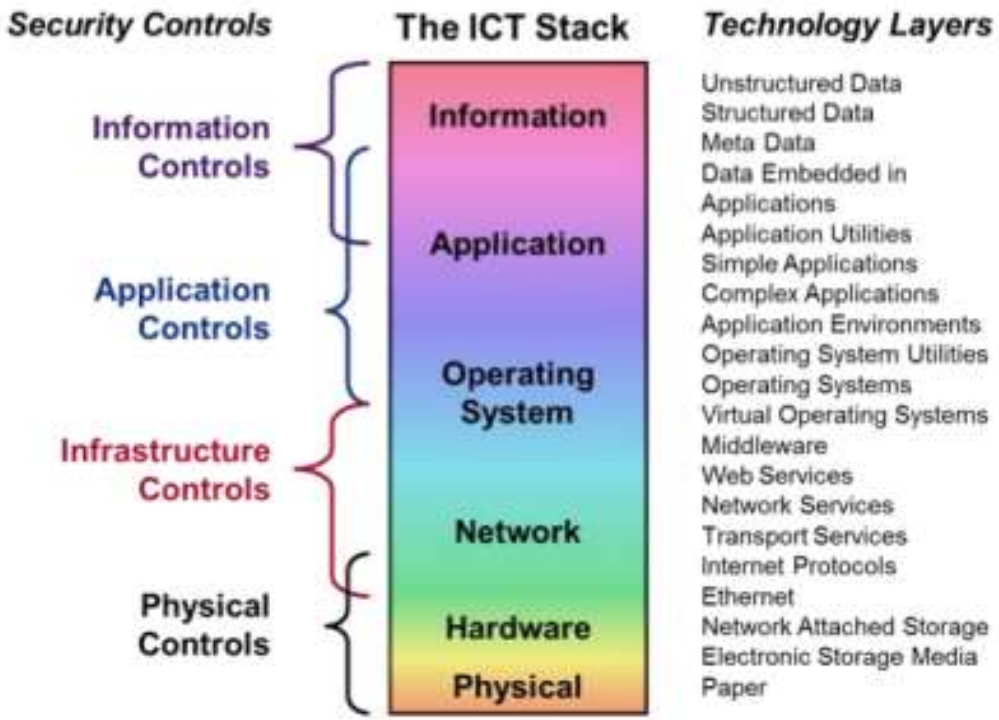
- как подключать к сети
- как аутентифицировать и авторизовывать
- какие ресурсы доступны и при каких условиях
- как не утратить контроль полностью
- какие риски мы должны принять

Харденинг и патчинг всего как образ жизни

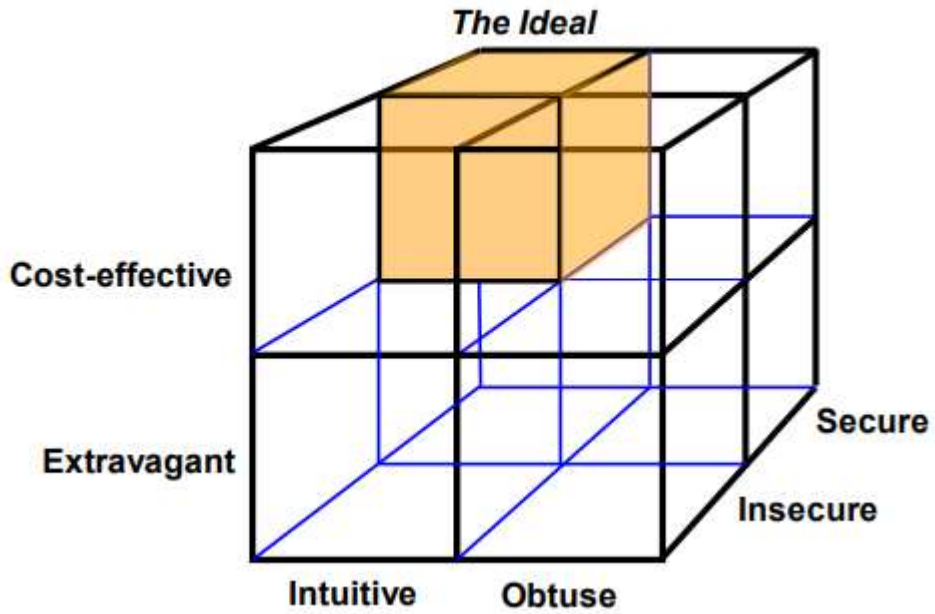
- 300+ субтехник MITRE ATT&CK закрывает харденинг в одиночку
- В сканере безопасности всегда все покрашено в красный цвет, но важно лишь то, что требует ручного управления
- Уверены, что работает? Пусть проверят пентестеры.

- Харденинг и патчинг - это точно бесплатно?

Эшелонированная защита – это не про разные антивирусы



Вы что-то говорили про риск-ориентированный подход




Q&A