Возможно ли на 100% защититься от киберугроз?

Спектакль в 2 актах.

Докладчик: Вячеслав Касимов, Иван Шубин

МОСКОВСКИЙ КРЕДИТНЫЙ БАНК

От хорошего к великому — один Банк

Акт 1.

Да! Конечно можно.*

*при наличии безлимитных ресурсов и в теории

С чего начать?

Устранение уязвимостей	Контроль доступа администраторов	Харденинг платформ
Надежная аутентификация	Мониторинг	Защита периметра
Защита от вредоносного ПО	Контроль целостности	….

Для приверженцев стандартов

МОСКОВСКИЙ КРЕДИТНЫЙ БАНК

Для приверженцев австралийских стандартов

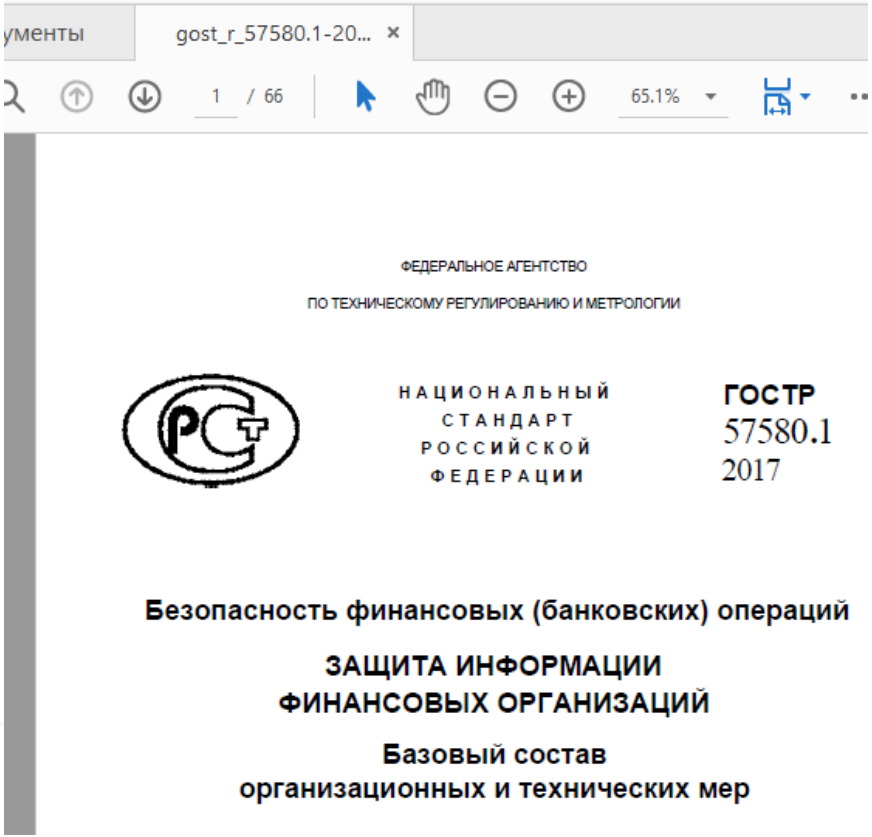
Au-DSD Top 35 Mitigation Strategies (Part 1)

Source: http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm

Ranking	Strategy
1	Patch applications within 2 days for high risk vulnerabilities.
2	Patch O/S within 2 days for high risk vulnerabilities.
3	Minimize the number of local admins. Assign separate accounts.
4	Application white-listing: Prevent unauthorized programs.
5	HIDS/HIPS: Identify anomalous behavior.
6	E-mail content filtering: Allow only authorized attachments.
7	Block spoofed e-mail.
8	User education.
9	Web content filtering.
10	Web domain white-listing.
11	Web domain white-listing for HTTP/SSL.
12	Workstation inspection of Microsoft Office files.

МОСКОВСКИЙ КРЕДИТНЫЙ БАНК

Для патриотов



МОСКОВСКИЙ КРЕДИТНЫЙ БАНК

Пример с криптографическим ключом на unix-сервере

Положим в контейнер

Исключим из мониторинга техническую УЗ

Контейнер зашифруем

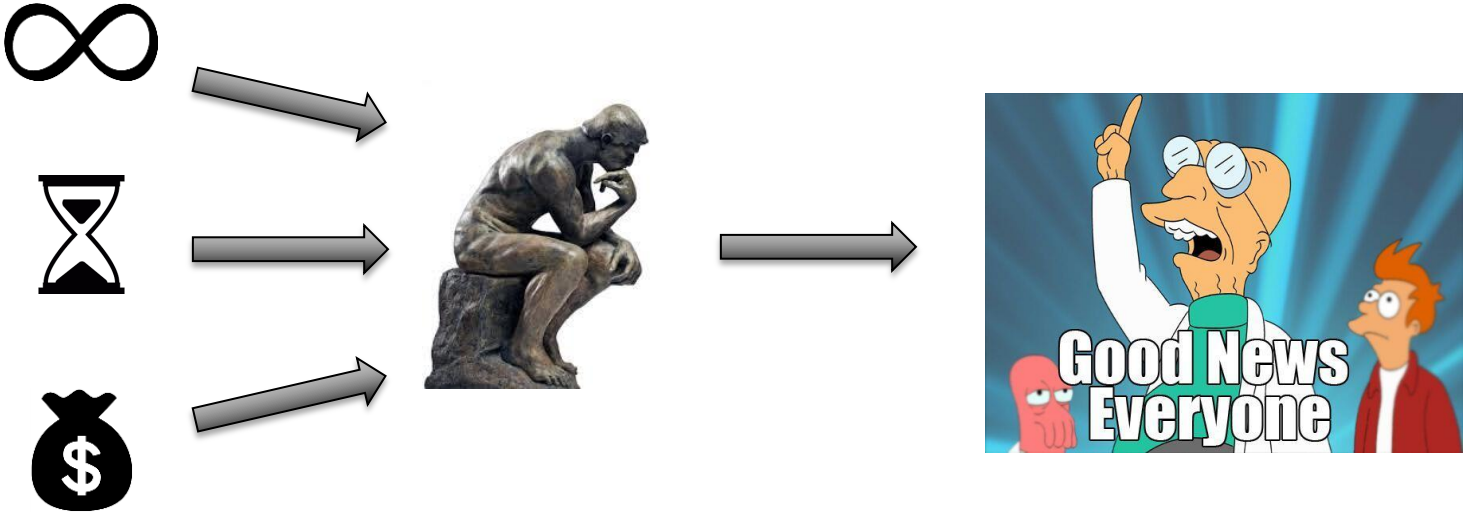
Просто в файле хранить нельзя

Machine learning + math.stat

Ключ для ключа размажем по среде ОС и ФС

Мониторинг доступа к ключу на чтение

Экономическая наука



Конец первого акта

Нет, Вы с ума сошли!

Вот это подойдет для начала

МОСКОВСКИЙ КРЕДИТНЫЙ БАНК

Рассмотрим один пример

SANS top 20

Critical Control		Effect on Attack Mitigation
1.	Inventory of Authorized and Unauthorized Devices	Very High
2.	Inventory of Authorized and Unauthorized Software	Very High
3.	Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High
4.	Continuous Vulnerability Assessment and Remediation	Very High
5.	Malware Defenses	High
6.	Application Software Security	High
7.	Wireless Device Control	High
8.	Data Recovery Capability	Moderately High to High
9.	Security Skills Assessment and Appropriate Training to Fill Gaps	Moderately High to High
10.	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately High
11.	Limitation and Control of Network Ports, Protocols, and Services	Moderately High
12.	Controlled Use of Administrative Privileges	Moderate to Moderately High
13.	Boundary Defense	Moderate
14.	Maintenance, Monitoring, and Analysis of Security Audit Logs	Moderate
15.	Controlled Access Based on the Need to Know	Moderate
16.	Account Monitoring and Control	Moderate
17.	Data Loss Prevention	Moderately Low to Moderate
18.	Incident Response Capability	Moderately Low to Moderate
19.	Secure Network Engineering	Low
20.	Penetration Tests and Red Team Exercises	Low

Тестирование

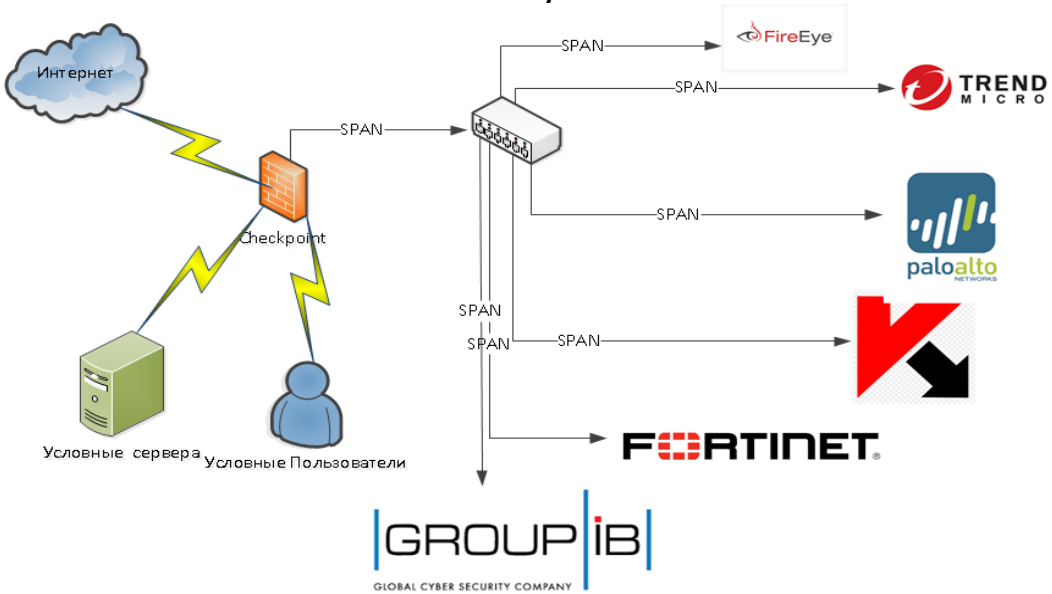
Здесь планировалась забавная картинка про разработчиков из Индии, но не получилось 😔

Нам понадобится:

1. Много трафика
2. «Надувной» домен
3. 500 новых «вирусов»
4. Логика
5. Фантазия (это самое главное)

Тестирование и результаты

ПиМ производителя – это не более чем проверка заявленного функционала…
какая скукота…



Результаты

Happy end!