R-Vision
At the root of your security

ЭВОЛЮЦИЯ SOAR: АВТОМАТИЗАЦИЯ ИБ ВЧЕРА, СЕГОДНЯ И ЗАВТРА

www.rvision.pro

Всеслав Соленик

Заместитель директора Центра экспертизы

ВЗГЛЯД В БУДУЩЕЕ

2024 – Элементы компьютерного интеллекта
станут обязательными в автомобилях.
Людям **запретят садиться за руль** автомобиля,
не оборудованного компьютерными помощниками

2025 – Появление массового рынка
гаджетов-имплантатов

2038 – **Появление роботизированных людей**, продуктов трансгуманистичных технологий. Они будут оборудованы дополнительным интеллектом (например, ориентированным на конкретную узкую сферу знаний, полностью охватить которую человеческий мозг не способен) и разнообразными опциями-имплантантами — от глаз-камер
до дополнительных рук-протезов.

Рэй Курцвейл, Google

ТЕНДЕНЦИЯ №1

Технологии усложняются и развиваются. Люди - нет

- **Недостаток квалифицированных кадров**
- **Несоответствие образования и технологий**
- **«Период полураспада» технологических знаний в сферах ИТ/ИБ оценивается специалистами в 1,5 — 3 года**
- **Объем информации vs. скорость принятия решения**

ТЕНДЕНЦИЯ №2

Текучка персонала

- **Людей переманивают (порой целыми командами)**
- **Специалисты выгорают**
- **Рынок становится «рынком соискателя»**

Опасное вместо

Банковские специалисты по кибербезопасности массово увольняются

Газета "Коммерсантъ" №117 от 08.07.2019, стр. 7

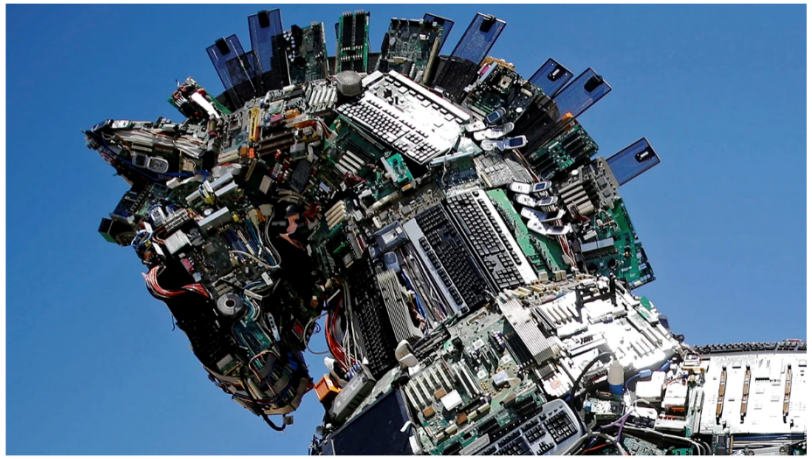


Фото: Amir Cohen / Reuters

Резко возросшие за последний год требования ЦБ к информационной безопасности привели к оттоку специалистов в этой сфере из банков в другие отрасли. Такая ситуация чревата рисками для банков и их клиентов, указывают эксперты: хакеры, которые в 2019 году переориентировали атаки с банков на госучреждения и промышленные компании, еще могут вернуться.

ТЕНДЕНЦИЯ №3

Стресс

Research Report: The Life and Times of Cybersecurity Professionals 2018 (https://tinyurl.com/y3vov37m)

КАК БОРОТЬСЯ

Обучение и удержание персонала

Автоматизация (SOAR)

Аутсорсинг (MSSP)

HR-брендинг

SOAR (by Gartner)

Было:

SOAR – security operations, analytics and reporting.

SOAR platform uses “machine-readable and stateful security data to provide reporting, analysis and management capabilities to support operational security teams.”

The three primary SOAR technologies are:

•**Threat and vulnerability management**, which supports the remediation of vulnerabilities across their lifecycle and provides formalized workflow, reporting and collaboration capabilities.

•**Security incident response**, which supports how an organization plans, manages, tracks, and coordinates the response to a security incident.

•**Security operations automation**, which enables the automation and orchestration of workflows, processes, policy execution and reporting.

Стало:

SOAR refers to **technologies that enable organizations to collect inputs** monitored by the security operations team.

For example, alerts from the SIEM system and other security technologies — where incident analysis and triage can be performed by leveraging a combination of human and machine power — help define, prioritize and drive standardized incident response activities.

SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format.

УРОВНИ АВТОМАТИЗАЦИИ

1 | Базовый: «Экзоскелет»

УРОВНИ АВТОМАТИЗАЦИИ

2 | Продвинутый: «Автопилот»

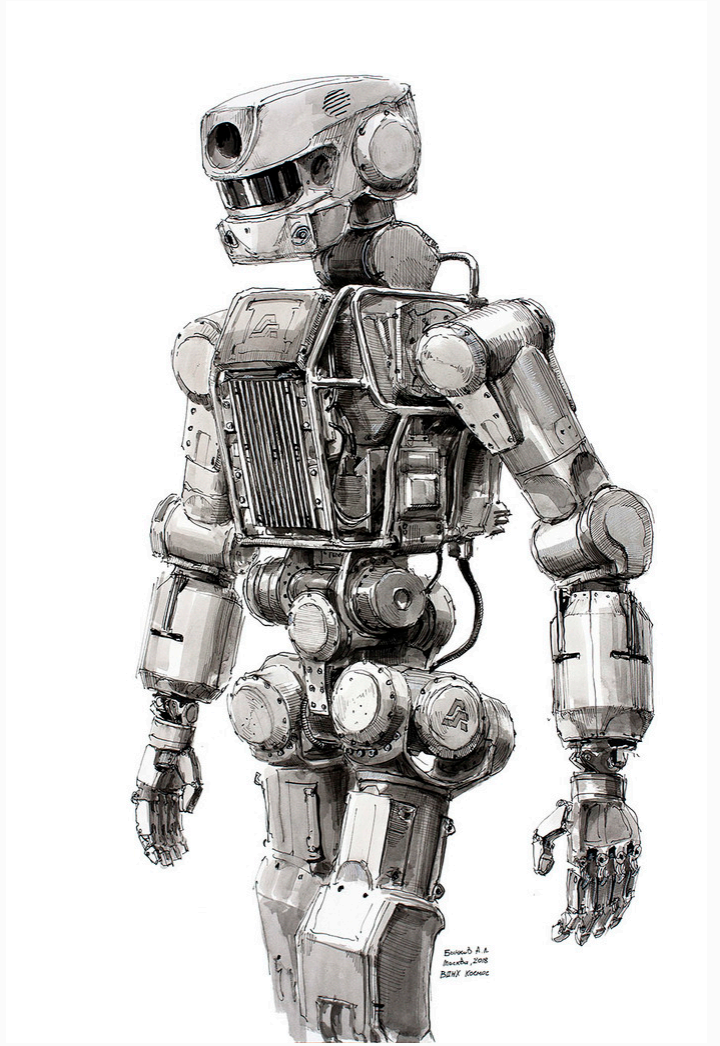
1 | Базовый: «Экзоскелет»

УРОВНИ АВТОМАТИЗАЦИИ

3 | **Перспективный: «Робот»**

2 | **Продвинутый: «Автопилот»**

1 | **Базовый: «Экзоскелет»**



АНТРОПОЛОГИЧЕСКОЕ ИССЛЕДОВАНИЕ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ SOC

June 2017

An Anthropological Study of Security Operations Centers to Improve Operational Efficiency

Sathya Chandran Sundaramurthy
University of South Florida, sathya.chandran3@gmail.com

https://tinyurl.com/y35ajsk4

АНТРОПОЛОГИЧЕСКОЕ ИССЛЕДОВАНИЕ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ SOC

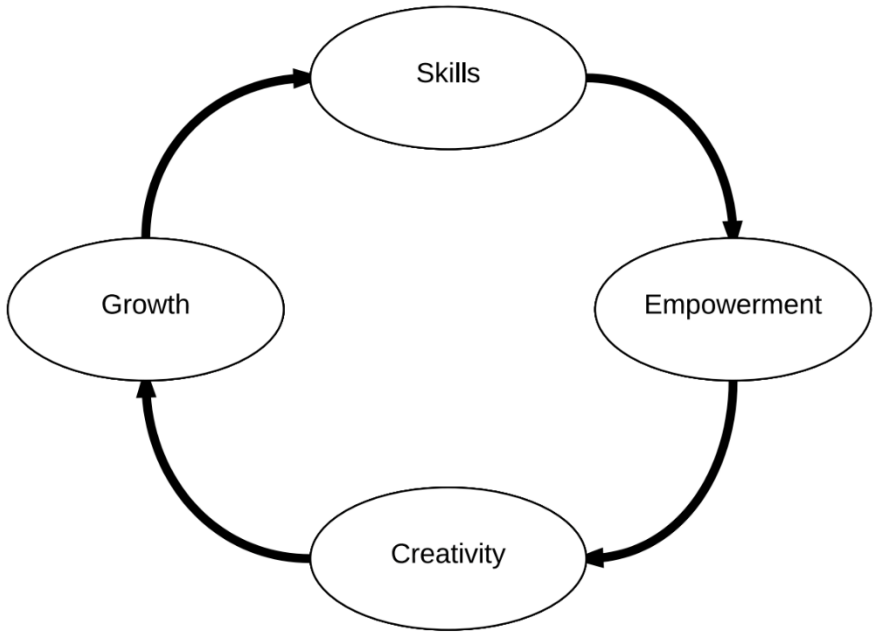


Figure 5.1: Human Capital Cycle

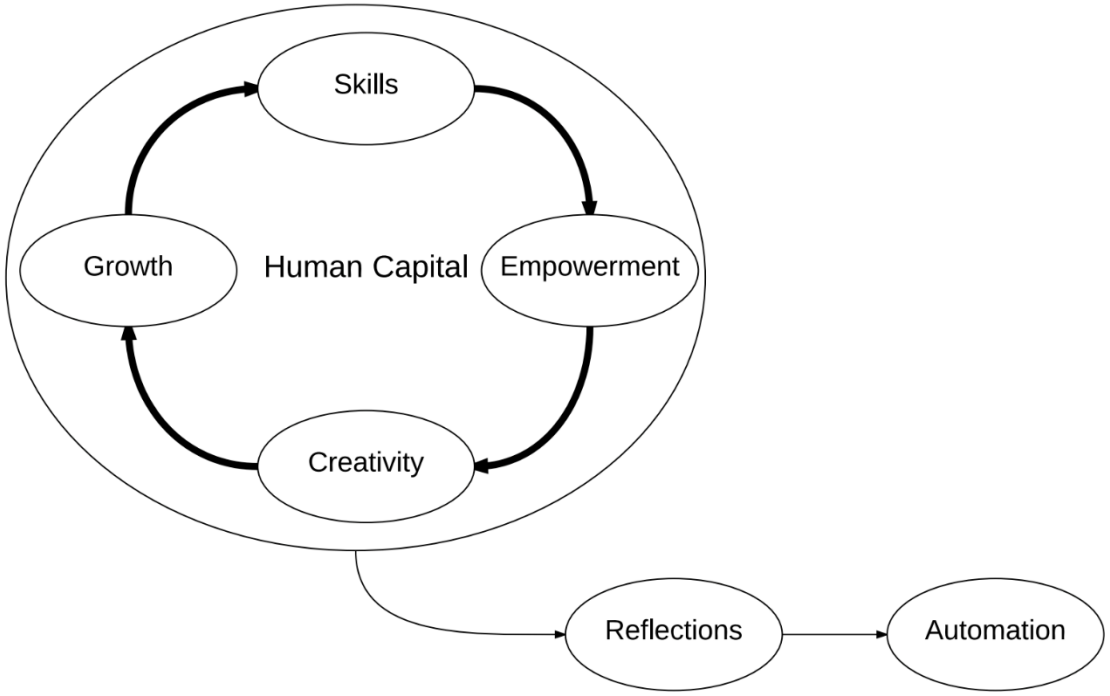


Figure 5.3: Automation

ПОДХОДЫ К АВТОМАТИЗАЦИИ

Автоматизация вчера

Эффективное управление активами и библиотекой документов

Определение алгоритмов обработки типовых ситуаций

Наведение порядка в процессах выявления и реагирования на инциденты

ПОДХОДЫ К АВТОМАТИЗАЦИИ

Автоматизация сегодня

Автоматизация мониторинга / поиска фактов компрометации

Кейс: TIP + SOAR + Honeypot

Автоматизация процессов ИБ (не только реагирования)

Автоматизация Compliance-контроля (технический аудит)

ПОДХОДЫ К АВТОМАТИЗАЦИИ

Автоматизация сегодня

Автоматизация мониторинга / поиска фактов компрометации

Кейс: TIP + SOAR + Honeypot

Автоматизация процессов ИБ (не только реагирования)

Кейс: Активы | Уязвимости | Риски

Автоматизация Compliance-контроля (технический аудит)

ПОДХОДЫ К АВТОМАТИЗАЦИИ

Автоматизация сегодня

Автоматизация мониторинга / поиска фактов компрометации

Кейс: TIP + SOAR + Honeypot

Автоматизация процессов ИБ (не только реагирования)

Кейс: Активы | Уязвимости | Риски

Автоматизация Compliance-контроля

Кейс: автоматический технический аудит

ПОДХОДЫ К АВТОМАТИЗАЦИИ

Будущее автоматизации

Автоматизация межотраслевая и междисциплинарная (RPA)

«Доверься мне, я машина!»

Автоматизация by design

Инкапсуляция и полиморфизм для автоматизации ИБ

Автоматизация процесса автоматизации

ПОДХОДЫ К АВТОМАТИЗАЦИИ

Вчера, сегодня и завтра

Автоматизация процессов – как культура компании, KPI, образ мысли.

Наряду с цифровизацией, Lean6Sigma, BPM, etc.

МЕТРИКИ

Эффект автоматизации может и должен быть посчитан

Среднее время обработки инцидента

Количество / тренды зафиксированных инцидентов vs. обработанных по SLA

Процент инцидентов, обработанных автоматически

ВЫВОДЫ

Автоматизация развивает и мотивирует персонал, а также нивелирует риски, связанные с текучкой, недостатком компетенций и ошибками

Основа: системный подход

Стратегия: движение от базового уровня к перспективному

Фокус на эффективности и результативности

Благодарю за внимание!

R-Vision
At the root of your security

Выпускаем регулярный Дайджест ИБ:
rvision.pro/blog

www.rvision.pro