MSS в концепции Zero Trust

Юрий Бармотин

Глобальная защита с локальной экспертизой

17 внутренних SOC по всему миру, выявляющие инциденты 24/7/365

11 коммерческих CyberSOC работающих совместно 24/7/365

4 CERT

4 центра очистки от DDoS атак

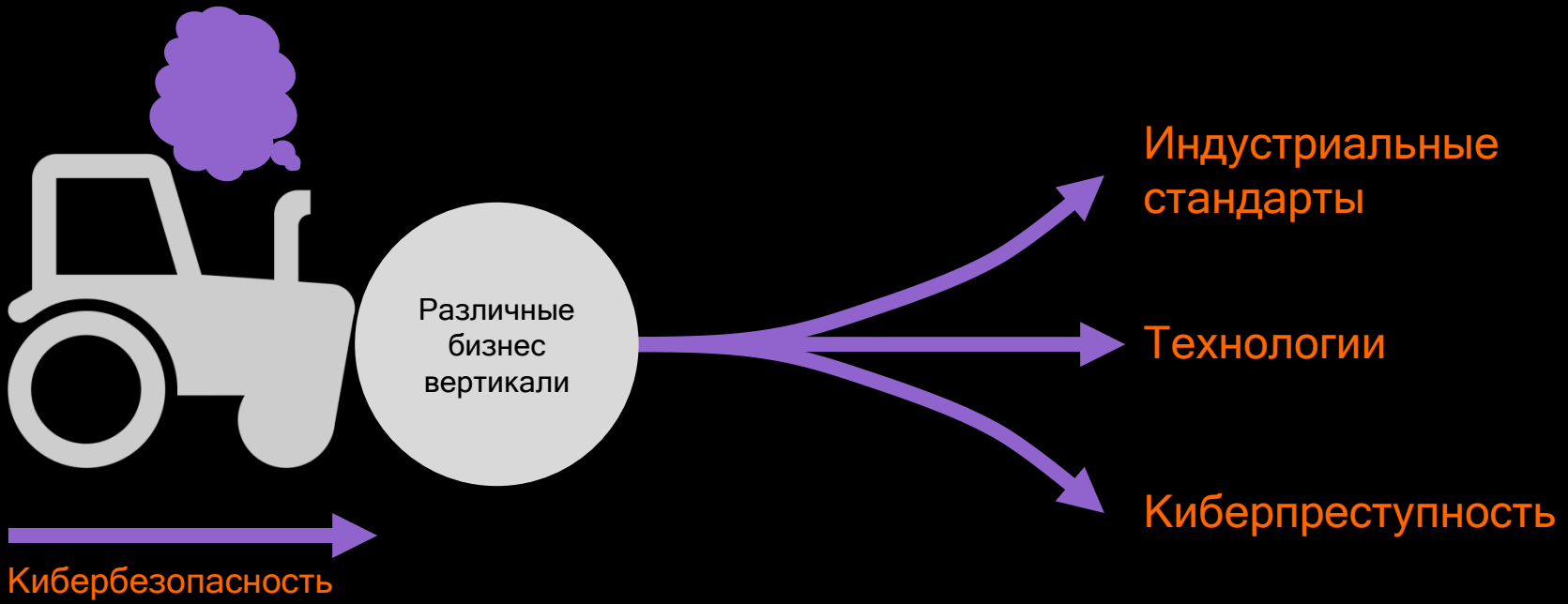
Собственный CERT

Реагирование на инциденты кибербезопасности

Расследования

Академия кибербезопасности

Катализаторы кибербезопасности

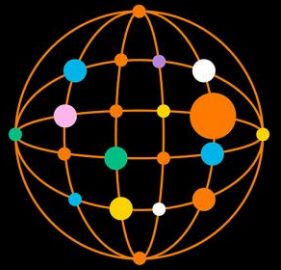


Индустриальные стандарты

К бизнесу предъявляются требования регуляторов, законодательства, индустриальных стандартов и т.д.

Например:

- Приказы ФСТЭК 17, 21
- СТО БР ИББС/ГОСТ 57580
- ФЗ 152, 187
- PCI DSS
- GDPR



Обеспечение соответствия порождает необходимость дополнительных финансовых затрат.

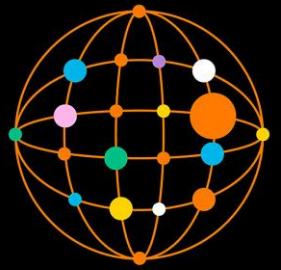
Технологии

Большинство приложений/транзакций работают через интернет

Переход «в облако» изменило представление о периметре сети

Теневой ИТ становится корпоративным ИТ

Индустрия 4.0 приносит вызовы и угрозы новых масштабов



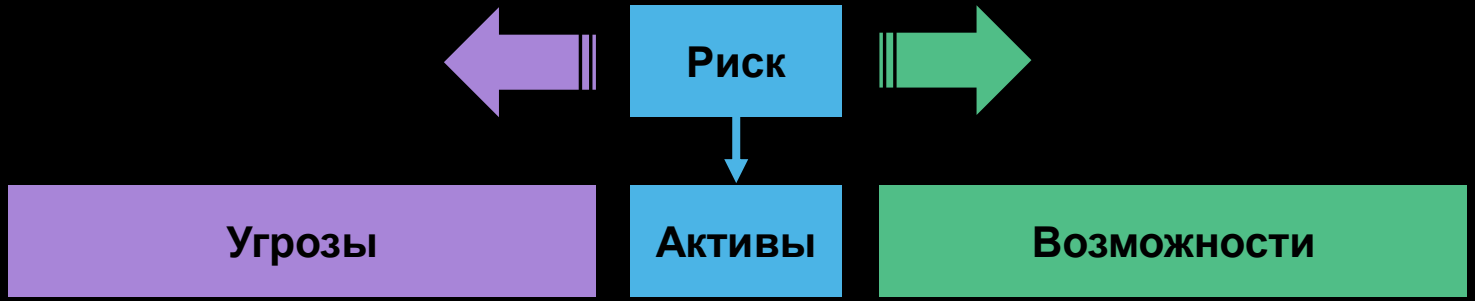
Киберпреступность

Киберпреступники организованы и финансово мотивированы

Киберпреступники меняют свои методы, чтобы использовать как технические, так и человеческие уязвимые места

Киберпреступники, имеющие не только финансовую мотивацию

Картинка всегда будет динамичной



- Безопасность – это баланс между удобством использования и защищенностью, между риском и возможностями
- Безопасность часто препятствует простоте использования

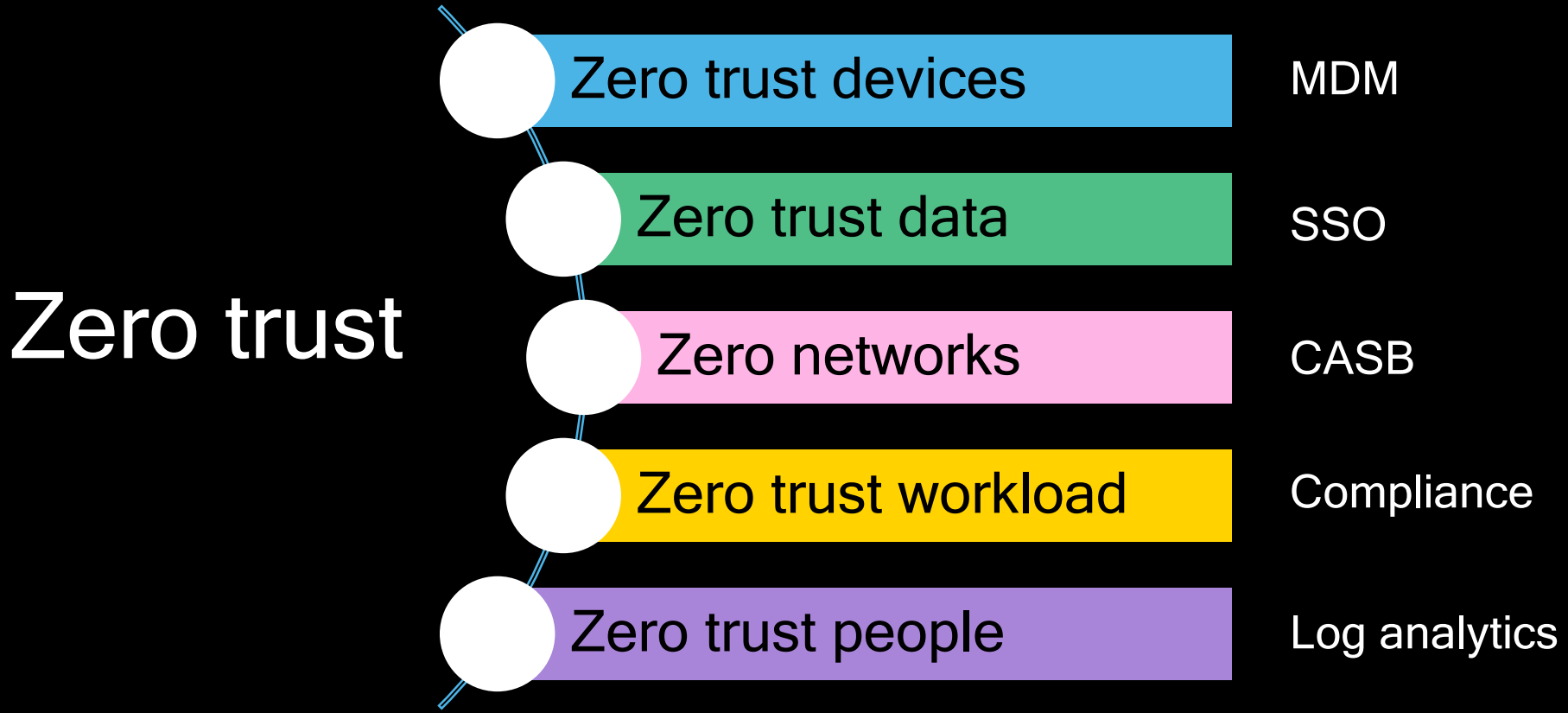
Концепция Zero Trust

Zero Trust – это концепция, которую разработал Джон Киндерваг в 2010 году.

Концепция заключается в том, что каждый пользователь или устройство должны подтверждать свои данные каждый раз, когда они запрашивают доступ к какому-либо ресурсу внутри или за пределами сети.

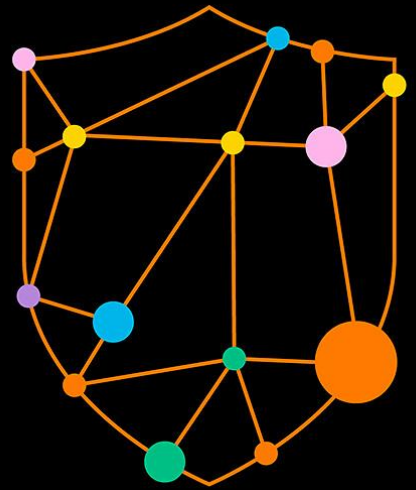
Фактически доверие изначально нулевое.

Из чего состоит концепция



Логические уровни концепции

- Процедуры
  - ИБ политики
  - Ревью кода
- Физический уровень
  - СКУД
  - Охрана
- Периметр
  - FW, NGFW
  - DDoS
  - DLP
- Сеть
  - TLS
  - Proxy
- Устройства и хосты
  - MDM
  - Vuln, mgmt
- Информация
  - Шифрование и защита информации



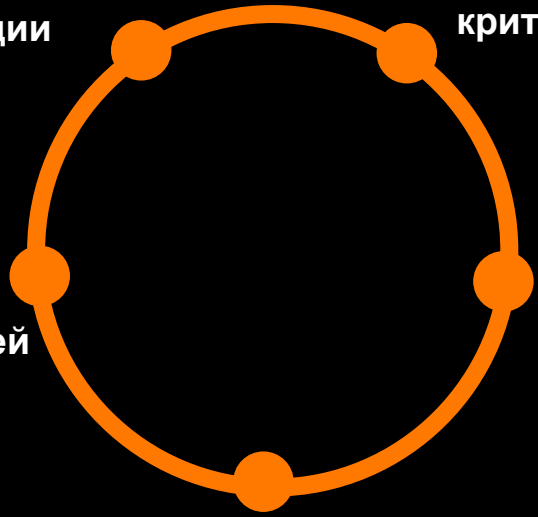
Принципы концепции

•Обеспечьте безопасный доступ к данным, оборудованию, системам и т.д. независимо от местоположения.

•Примите стратегию модели наименее привилегированного доступа и обеспечьте строгий контроль доступа: человеку должен быть предоставлен доступ только к ресурсам, необходимым для выполнения его работы, и запрещен доступ к остальным.

•Проверяйте и записывайте все: активность следует проверять не только при доступе к сети, но и внутри, пытаясь выявить ненормальное поведение.

Как внедрять концепцию



1 Идентифицируйте свои критичные активы

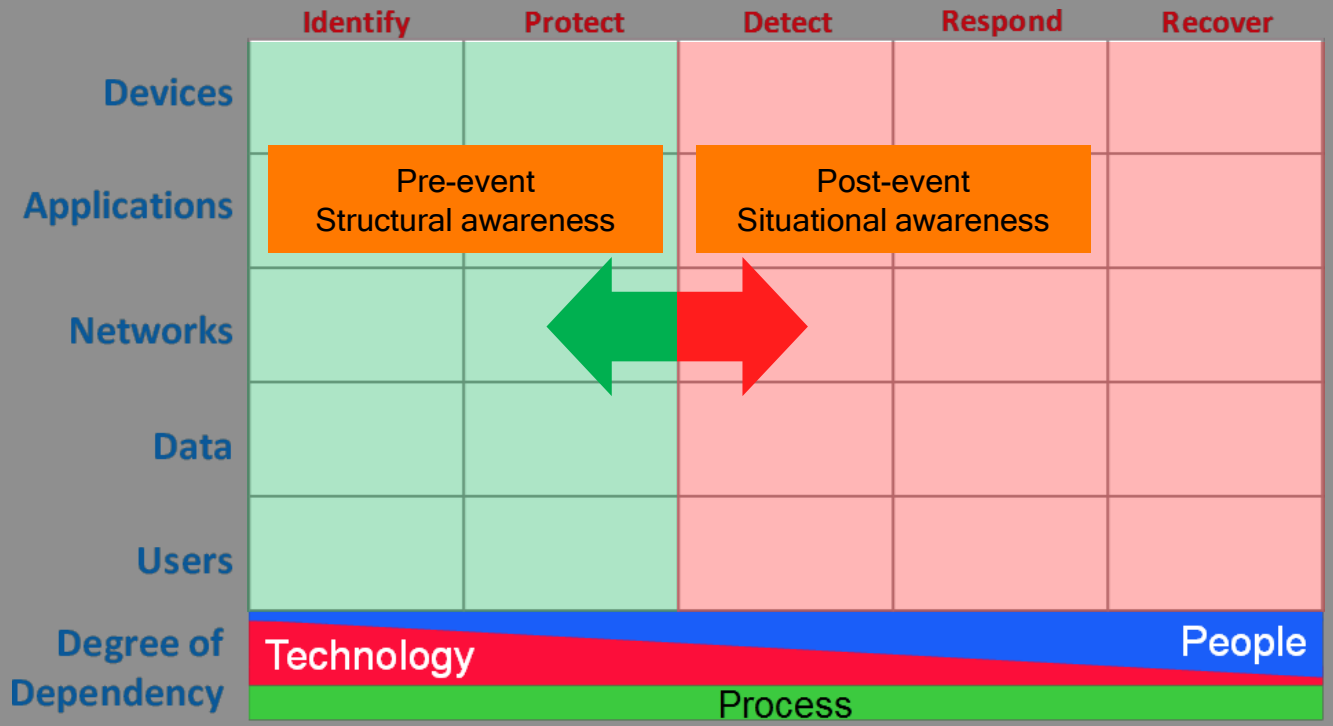
2 Проанализируйте процесс прохождения критичной информации в компании

3 Выделите ZT ИБ периметры

4 Непрерывно занимайтесь мониторингом всей экосистемы ZT

5 Внедряйте системы автоматизации

OWASP Cyber Defense Matrix



Как работает CyberSOC

SOC сервисы

- Log collection
- Monitoring and detection
- Incident response and remediation
- Customer Portal with Incident Reports

Дополнительно к SOC

- Managed Threat Response (Isolation/Takedown)
- Managed Vulnerability Intelligence (watch)

Управляемые сервисы

- Managed Firewall
- Connectivity encryption
- Internet Umbrella (DDoS Protection)
- Site Guardian (DDoS Protection)
- Security Awareness
- Security Audit
- Vulnerability Watch (CERT)

Процесс работы над инцидентами

SOC	Команда ИБ	Команда ИТ
Оповещение ИБ команды	Принятие инцидента в работу	
Сбор информации	Анализ инцидента	
Предоставление рекомендаций	Оповещение ИТ команды	Принятие инцидента в работу
	Проверка устранения	Устранение инцидента
	Проверка устранения	Результаты устранения
Закрытие инцидента	Результаты устранения	

Технологический стек, люди, экспертиза

Инфраструктура

- Tier III/Level 3 ДЦ МСК
- Своя платформа виртуализации с ISO27K
- Zero trust network segmentation
- Лицензии ФСТЭК (SOC)
- Выделенные NGFW под каждого заказчика
- Изолированные среды Prod/Dev/Demo
- Выделенные events storage node под каждого заказчика
- Cyber resilient Internet Uplinks
- Полностью «белая» инфраструктура (лицензии)
- Full data backups
- MPLS/IPSec SOC connectivity
- ГОСТ-шифрование каналов

Tools & Software

- SIEM IBM QRadar
- Threat Intelligence (multiengine)
- Protected Analysts Workspace
- Cisco Threat Grid
- Check Point Sandblast, NGTP
- Kaspersky endpoint security
- McAfee endpoint security

Люди

- L1 Analyst (3 года опыта)
- L2 Experts (+5 лет опыта)
- L3 Security консультанты (+5 лет опыта)
- Выделенный security manager
- Сертифицированные эксперты

Экспертиза

- Microsoft, Cisco, Oracle, Fortinet, Check Point, NetScout, Mobile Iron, Juniper, Huawei, VMware, DevOps
- Global expertise – IBM QRadar Skill Center, Orange CERT

Delivery

- Use-case and playbook catalogs relevant for different business verticals
- Design/Build/Run delivery model
- MSSP Infrastructure ready for onboarding
- PoC SOC ready for onboarding
- Project & Service Governance

Спасибо

Юрий Бармотин yury.barmotin@orange.com

orange™ Business Services