SOC: внутрь процессов

Юрий Бармотин
yury.barmotin@orange.com

orange™ Business Services

Наша agenda на сегодня

1. Создание
2. Процессы
3. Команда

Полезная информация

наш опыт

Советы

Заблуждения

Настоятельно рекомендуется

Группа Orange: возможности глобального лидера

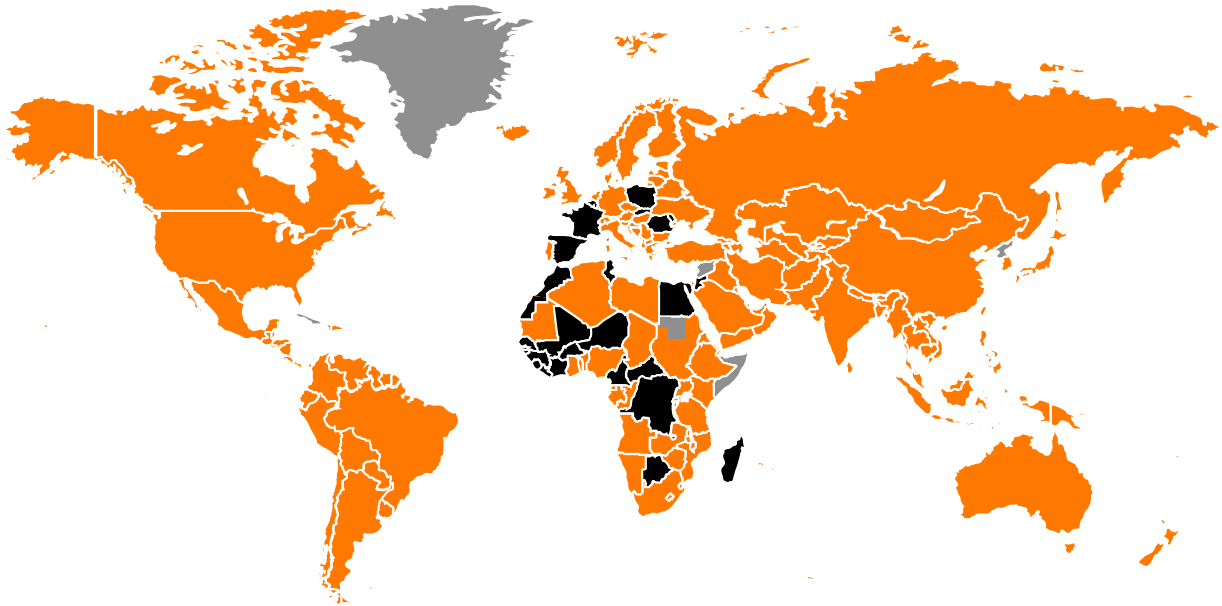
273+ млн
клиентов

€41,1 млрд
выручка в 2017 году

450 000 км
подводных кабелей

€600 млн
ежегодных инвестиций в магистральную инфраструктуру

345 000+ точек подключения
уникальное покрытие по всему миру



- Крупнейшая в мире бесшовная сеть передачи голоса и данных с предоставлением сквозных услуг связи. Сотрудники в 220 странах и территориях
- Оператор связи для населения в 29 странах
- Нет присутствия Orange Business Services

Orange в России

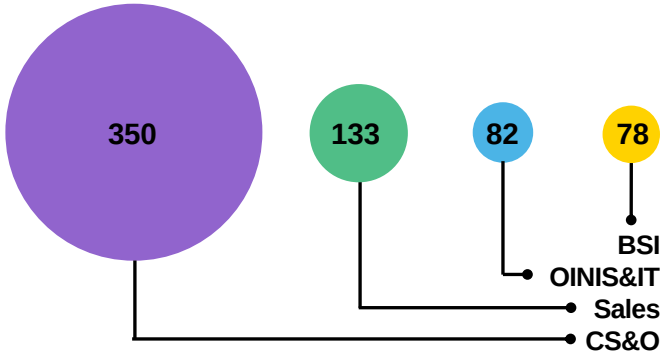
B2B-подразделение группы Orange: провайдер цифровых сервисов с экспертизой в области телекоммуникаций

Единственный международный оператор связи с собственной инфраструктурой

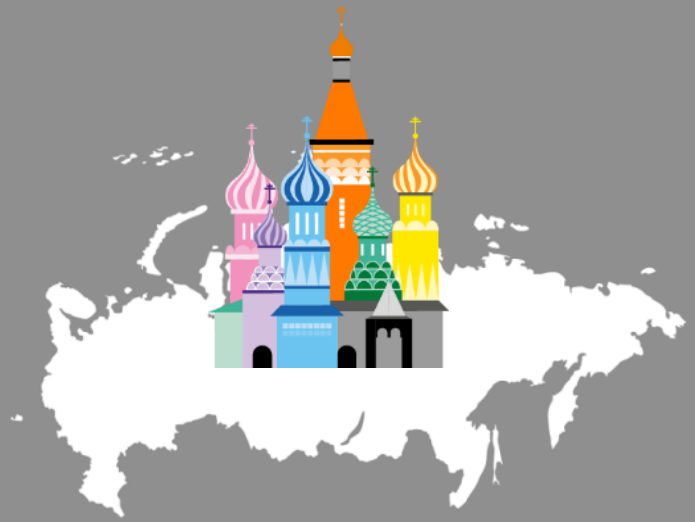
Присутствуем в 220 странах и территориях

Сильные местные компетенции: центр инноваций и центр мониторинга киберугроз (SOC)

Создаем инновации для крупного бизнеса: 8 из 10 крупнейших российских компаний Forbes-2000 Top-10 – наши клиенты*



800+ сотрудников



В России с 1958 года (SITA)

- **31 отделение**
- **13 офисов продаж**
- **1500 корпоративных клиентов**

*according to Top-2000 Forbes 2018 rating

Глобальное присутствие по направлению ИБ

- **Независимый CERT**
- **Реагирование на инциденты ИБ**
- **Форензика**
- **Академия кибербезопасности**

- 4 CyberSOC : корреляция событий, реагирование на инциденты 24x7x365
- 8 SOC : управление устройствами безопасности 24x7x365
- 3 CERT : реагирование и расследование инцидентов ИБ 24x7x365
- 3 scrubbing centers : защита от DDoS атак 24x7x365

С чего все начиналось?

Нужно учитывать

Опыт в информационной безопасности

Мониторинг инцидентов

плюс 1-2 года

Организация сменной работы

Создание SOC

Cloud computing risks

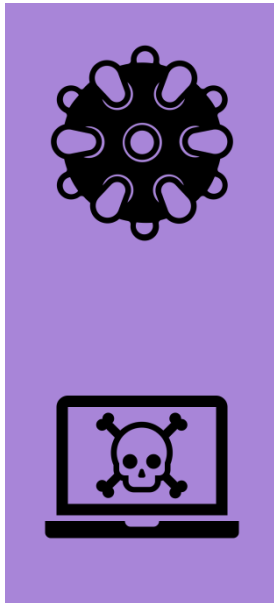
Data breaches
Insufficient identity, credential and access management
Insecure interfaces and APIs
System vulnerabilities
Account hijacking
Malicious insiders
Advanced Persistent Threats
Data loss
Insufficient due diligence
Abuse and nefarious use of Cloud Services
Denial of service
Shared technology vulnerabilities

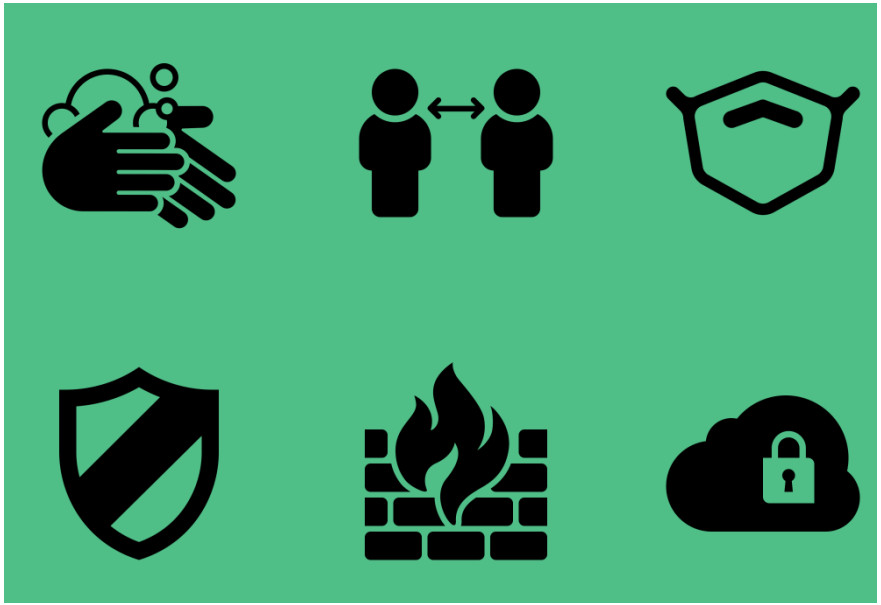
Top Threats to Cloud Computing – Cloud Security Alliance

Physical security
Access controls
Logging and monitoring
Host hardening
Patching
Vulnerability scanning
SDLC
Penetration testing
Risk modeling
SSO
RBAC
Audit logs
Data encryption
Data governance
Backups (data and systems)

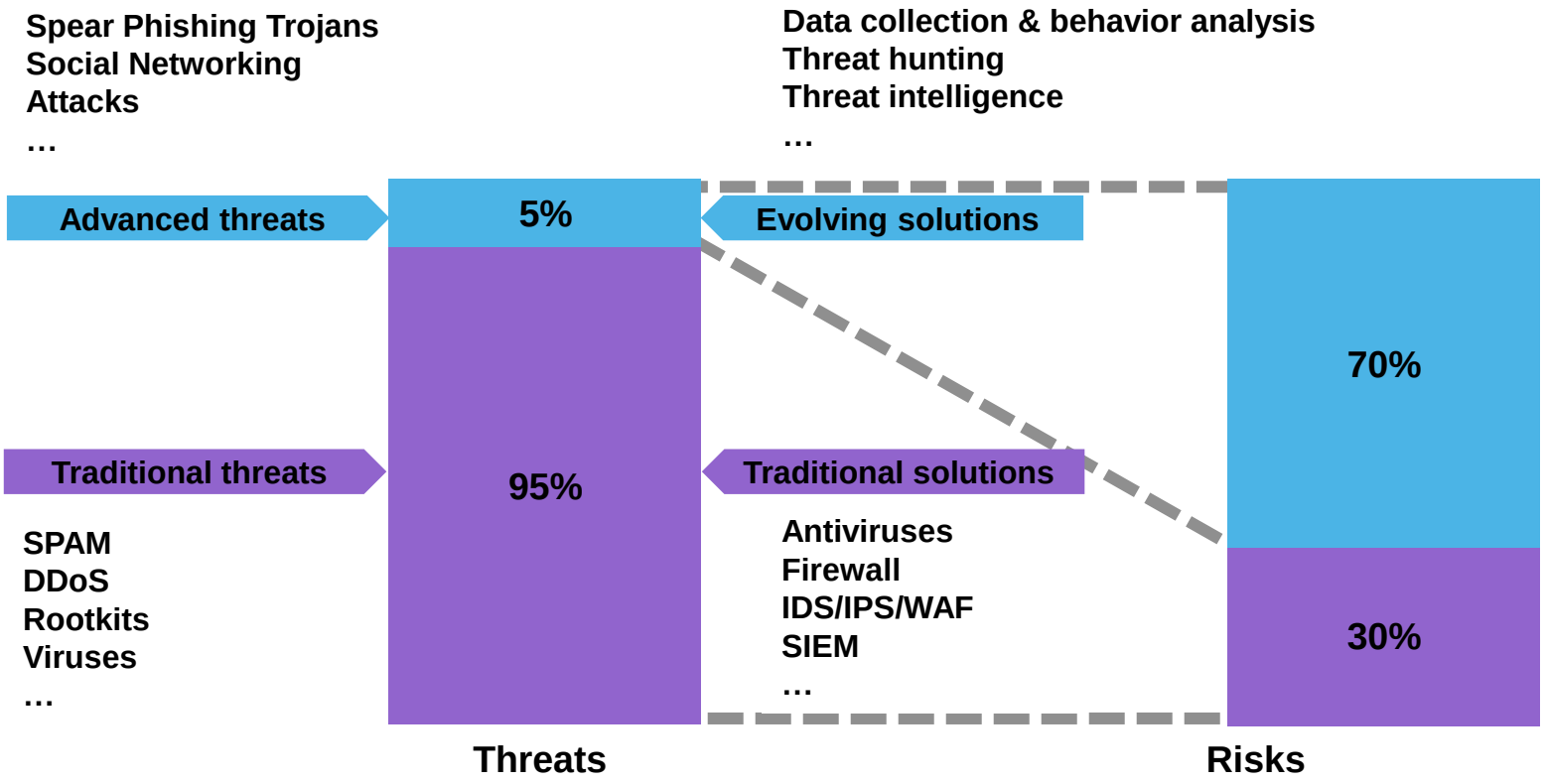
Defense in Depth proposed by Databricks on Azure provide following controls to mitigate risks

Если провести аналогию





ИБ Мониторинг. Для чего он нужен?



Типичная картина

- **85 различных инструментов ИБ**
- **45 вендоров**
- **83% заказчиков не видят уязвимостей в системах безопасности**

*IBM

Cybersecurity framework v.1.1.

1. **Оценить текущее положение ИБ;**
2. **Описать целевое состояние ИБ;**
3. **Выявить и расставить приоритеты возможных улучшений в непрерывном процессе улучшения и развития;**
4. **Оценка прогресса по достижению целевого состояния;**
5. **Информирование внутренних и внешних заинтересованных сторон о рисках кибербезопасности.**

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Риски и как с ними быть?

Ядро Фреймворка состоит из пяти параллельных и непрерывных функций:

- **Идентификация – управление рисками кибербезопасности для систем, людей, активов, данных и возможностей**
- **Защита – разработка и внедрение защиты для критичных сервисов**
- **Обнаружение – разработка мер по выявлению инцидентов информационной безопасности**
- **Реагирование – принятие мер при обнаружении инцидентов информационной безопасности**
- **Восстановление – разработка и поддержка планов восстановления услуг и планов обеспечения непрерывности**

При совместном рассмотрении эти функции обеспечивают высокоуровневый стратегический взгляд на жизненный цикл управления рисками кибербезопасности в организации.

Примеры

Управление активами, оценка рисков, стратегия управления рисками

Управление доступом и учетными данными, повышение осведомленности и другие виды обучения сотрудников по ИБ, меры по защите данных бизнес процессов , техническое обслуживание систем

Работа с аномалиями и событиями ИБ, осуществление мониторинга ИБ

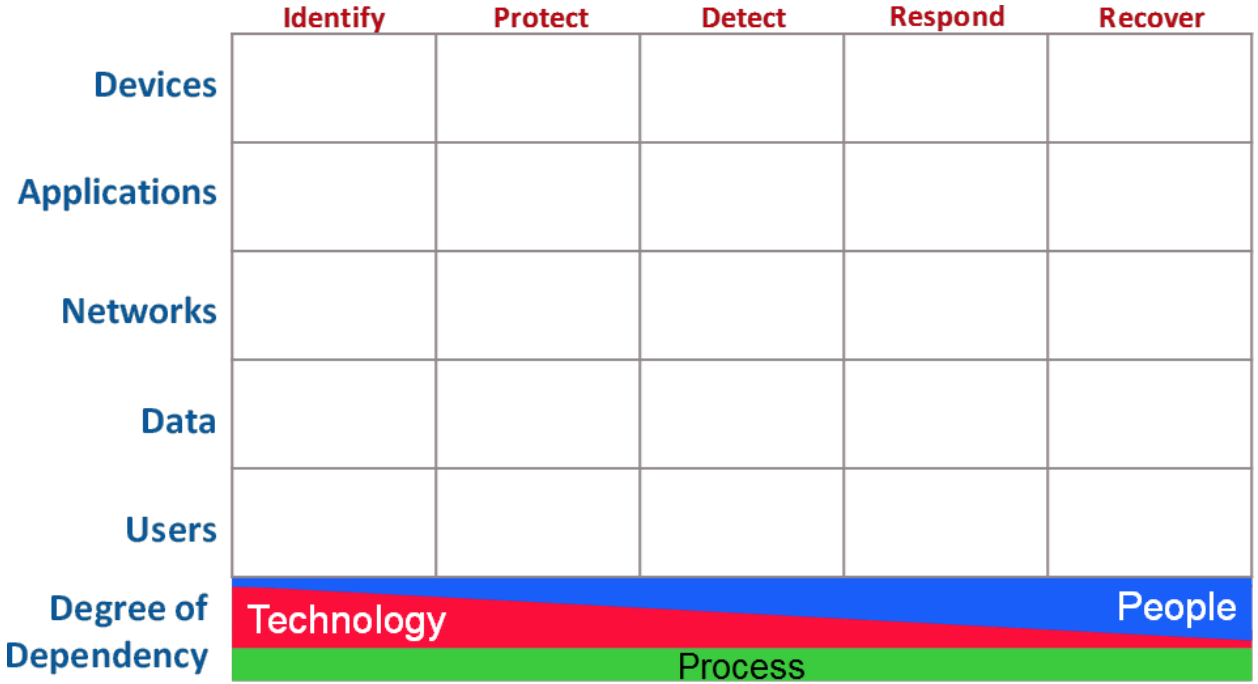
Процедуры по реагированию на инциденты ИБ, коммуникации, улучшения, анализ инцидентов ИБ, устранение инцидентов

Планы восстановления, улучшения, коммуникации

Как использовать Фреймворк

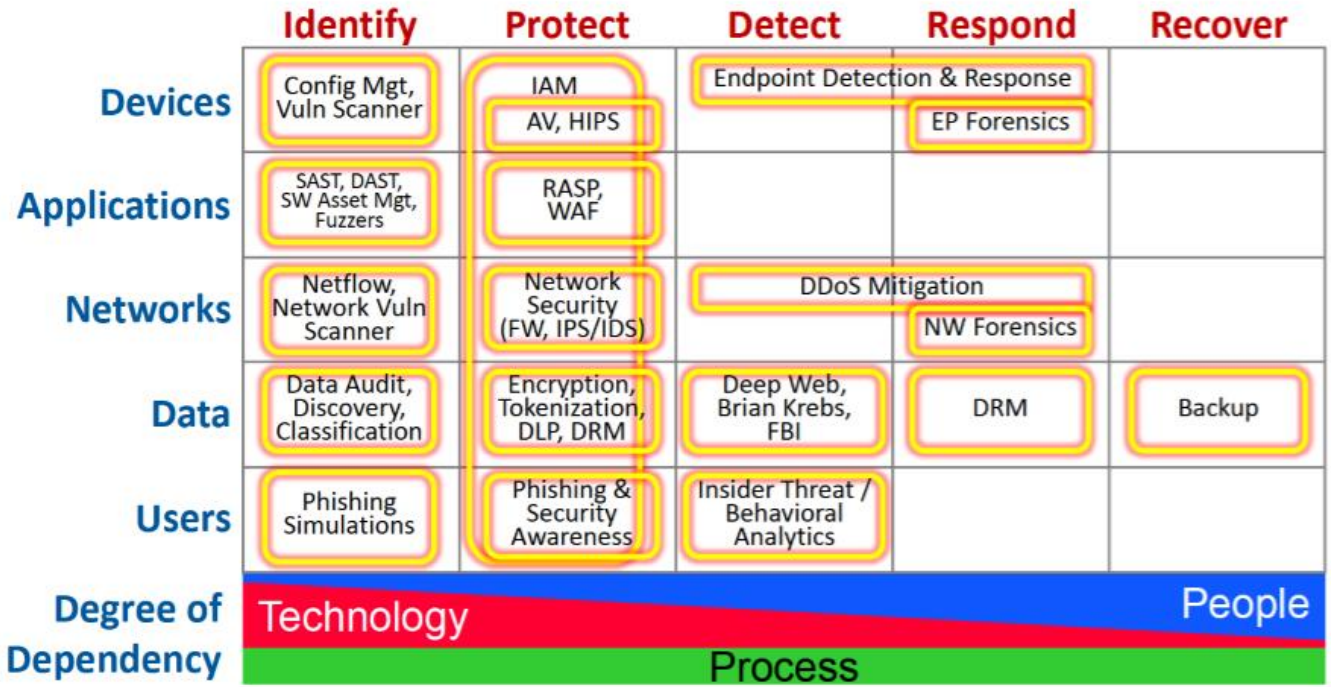
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

OWASP Cyber Defense Matrix



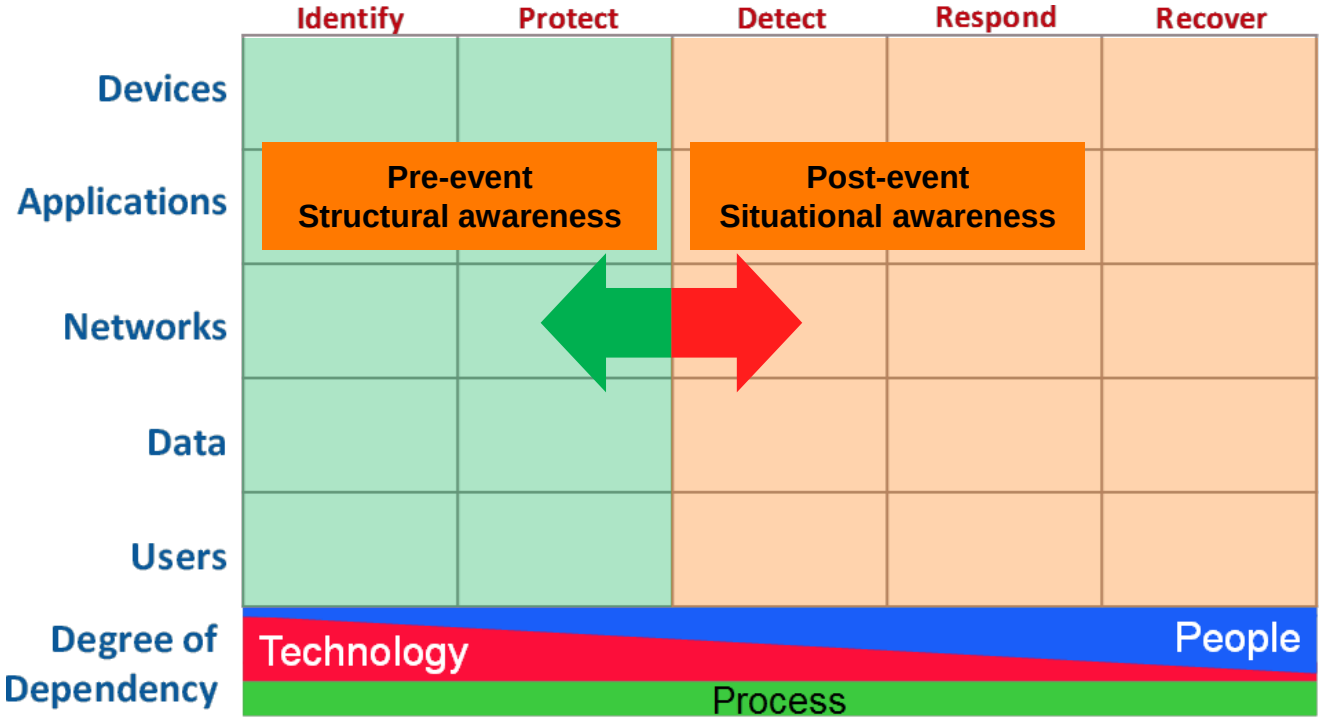
OWASP
Open Web Application Security Project

Enterprise security market segments



OWASP
Open Web Application Security Project

OWASP Cyber Defense Matrix

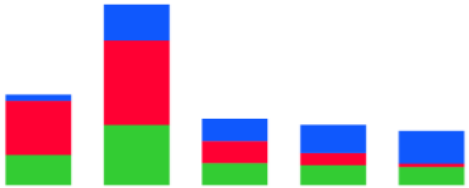


OWASP
Open Web Application
Security Project

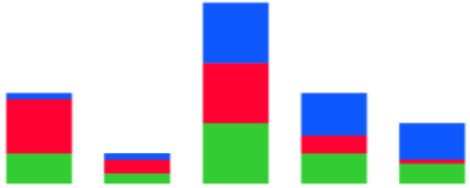
Рекомендуемые соотношения

	Identify	Protect	Detect	Respond	Recover
Technology	90	70	50	30	10
People	10	30	50	70	90
Processes	50	50	50	50	50
Tech:People Ratio	~10:1	~2:1	1:1	~1:2	~1:10

RISK ADVERSE POSTURE

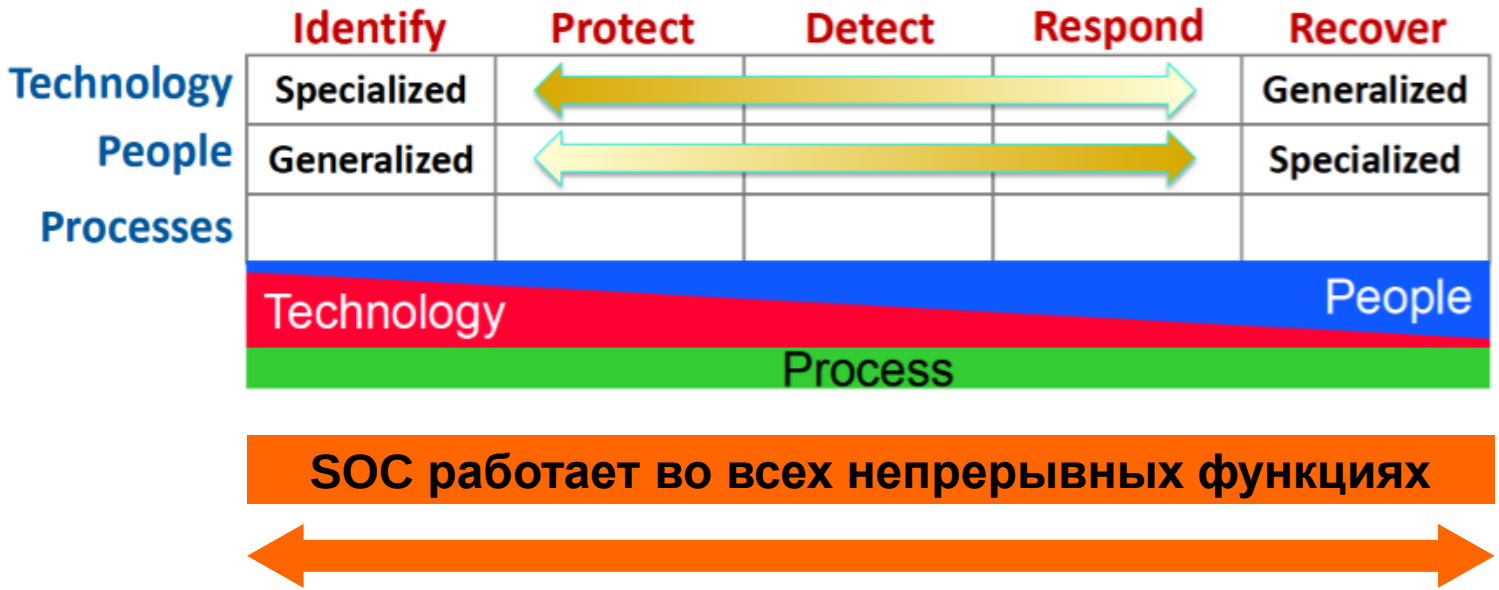


RISK TAKING POSTURE



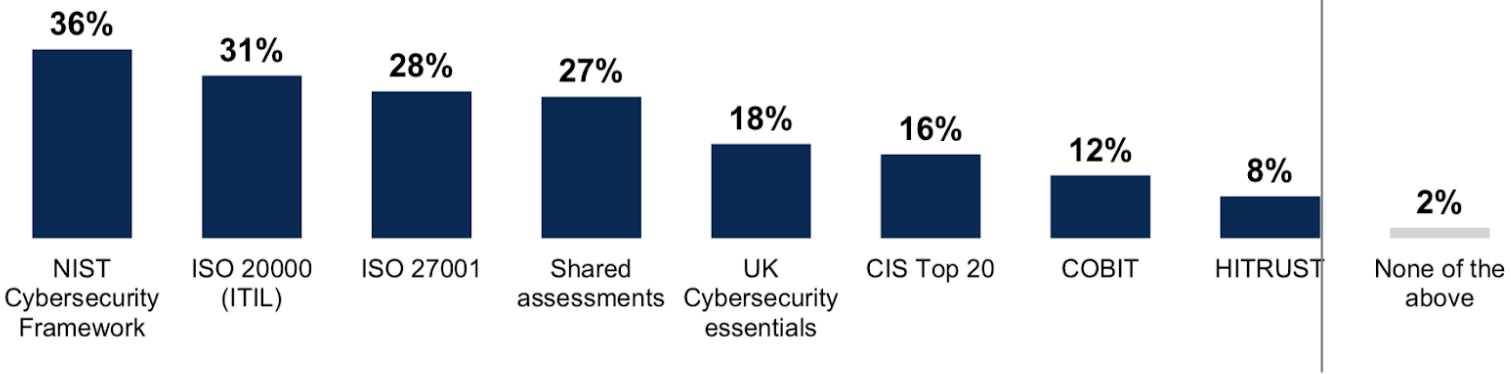
OWASP
Open Web Application Security Project

Навыки



Таблетки от всего не бывает

+ Приказы ФСТЭК 17/21/235/239
+ СТО БР ИББС/ГОСТ 57580
+ ГОСТ Р ИСО/МЭК 27001



Gartner

С чего начинался наш SOC

Firewalls

Web Security

Secure Internet Gateway

Endpoint Security

Malware Detection

Email Security

DLP

IPS

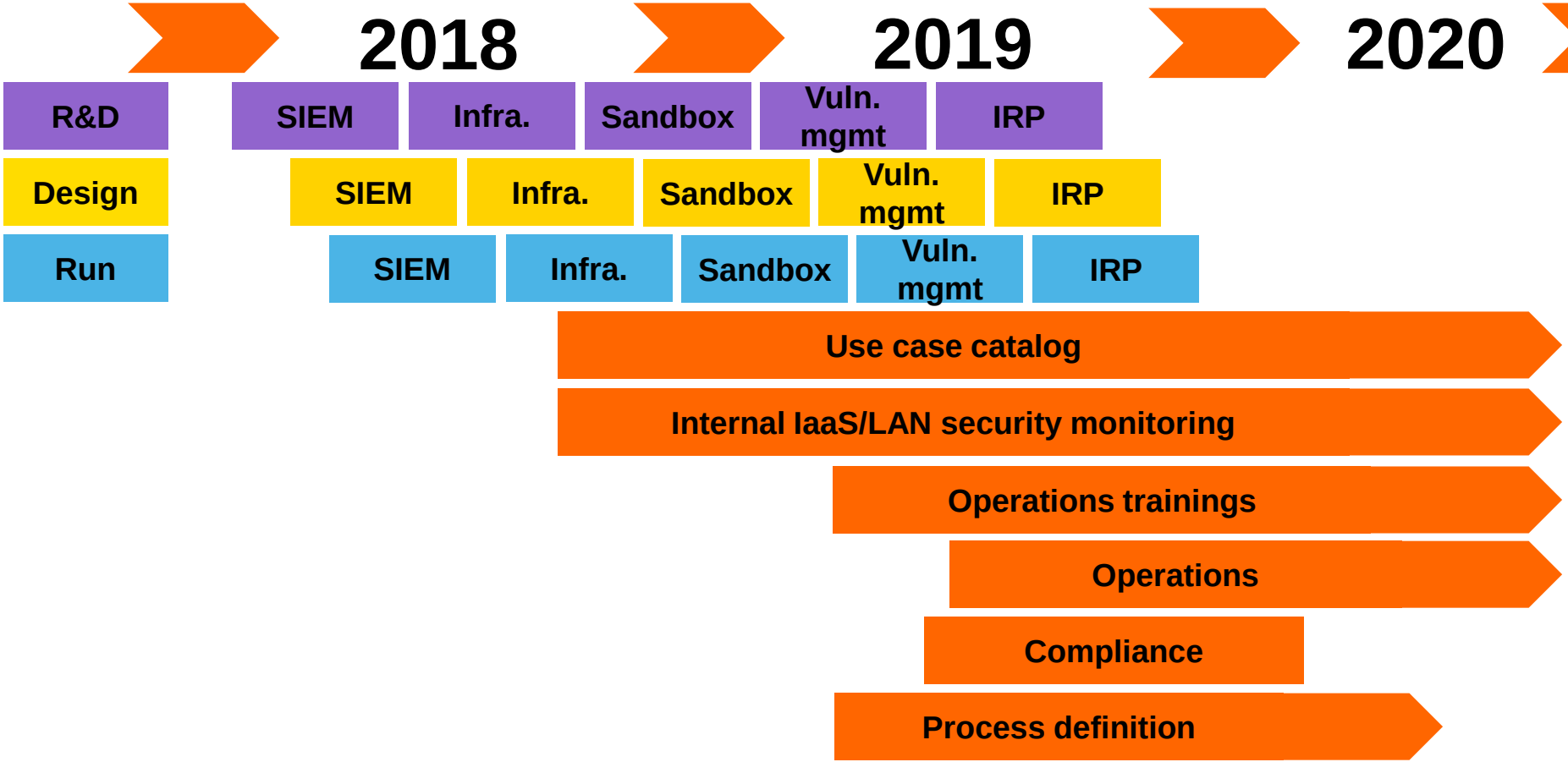
Из чего состоит SOC?

Technologies

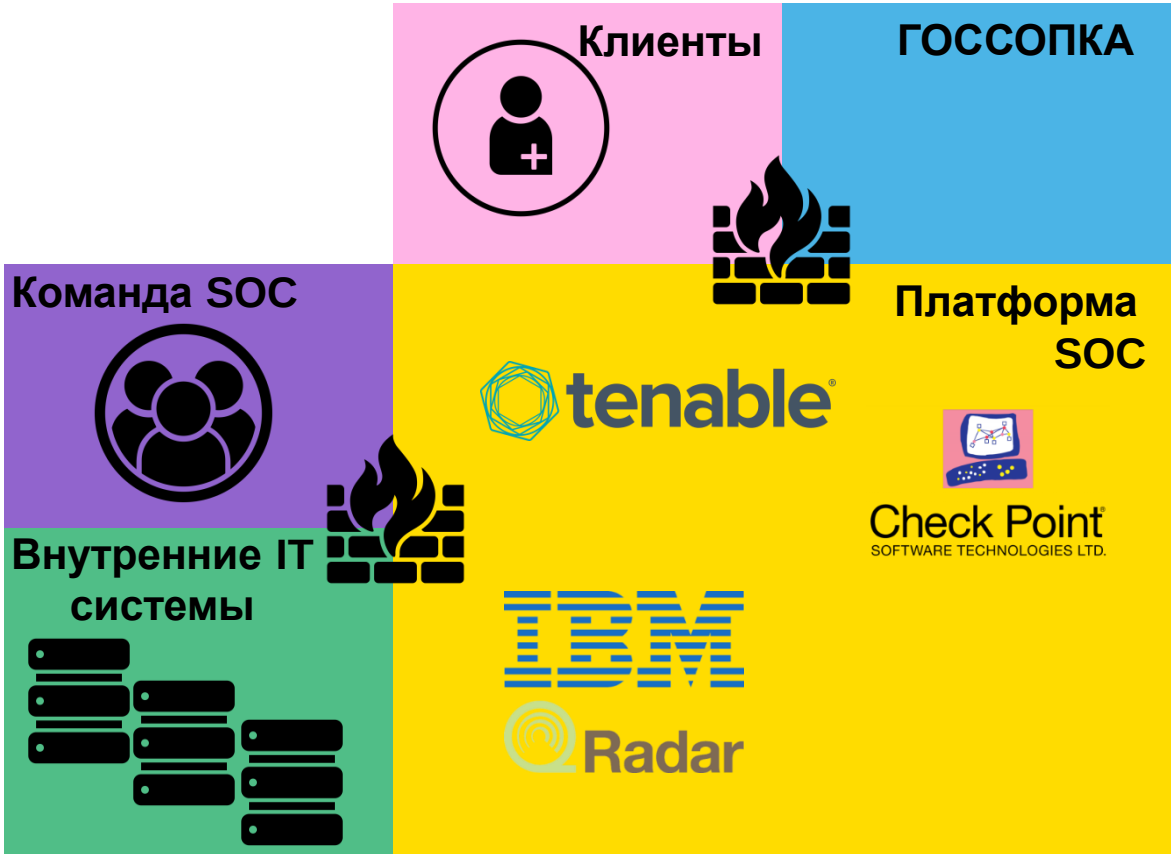
People

Processes

Как создавался SOC?



Логическая схема



- Выделенные сетевой сегмент
- Выделенный сетевой периметр под каждого клиента
- SIEM IBM Qradar в multitenant режиме
- Check Point Sandblast
- Сканнер уязвимостей Tenable
- Лицензионная «чистота»
- Обновленная инфраструктура

Создание SOC: советы и заблуждения

- Анализ рисков и анализ защищенности инфраструктуры
- Фреймворки
- Конференции и учения
- Ранее обучение команды поддержки
- Выделенная команда
- Внешний консалтинг

- SOC является решением всех проблем ИБ
- SOC является готовым коробочным решением
- Нужно заниматься мониторингом всего
- Внешний консалтинг построит под ключ SOC

- Цели и ключевые метрики успешности
- Постоянное взаимодействие и поддержка руководства.
- Загрузка участников рабочей группы.
- Выделенный PM.
- Базовый уровень защищенности инфраструктуры
- Повышение осведомленности сотрудников, периодическое обучение

Процессы в SOC

Типовой ввод в эксплуатацию

Prepare

- Консультация заказчика
- Организация единой схемы сбора событий ИБ
- Определение перечня источников событий
- Согласование способа передачи событий ИБ
- Подготовка инфраструктуры
- Подготовка инструкций для конфигурации источников событий

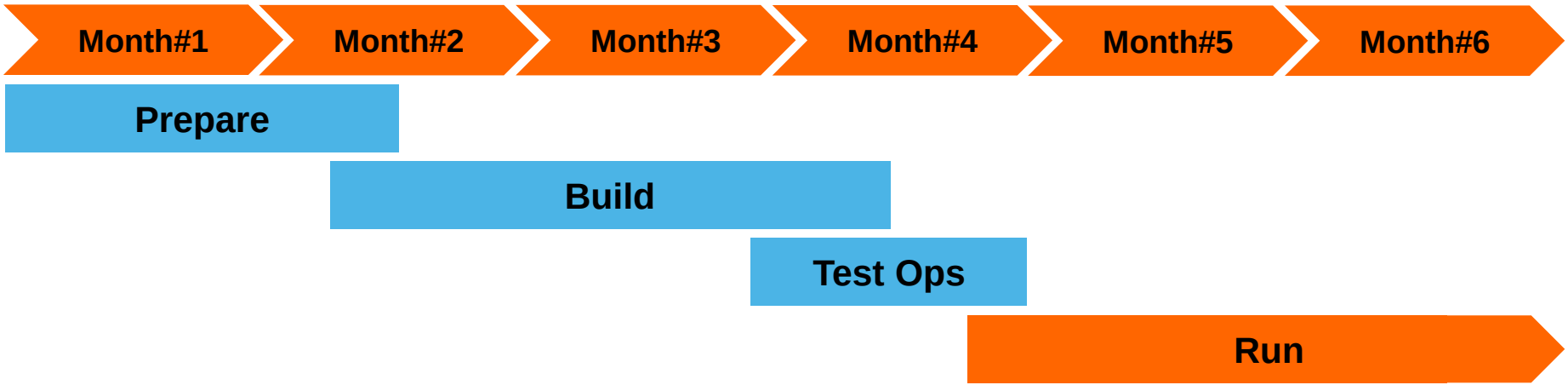
Build

- Настройка схемы сбора логов
- Подключение всех источников событий
- Модернизация схемы сбора событий ИБ
- Включение каталога use-case в соответствие с заданием

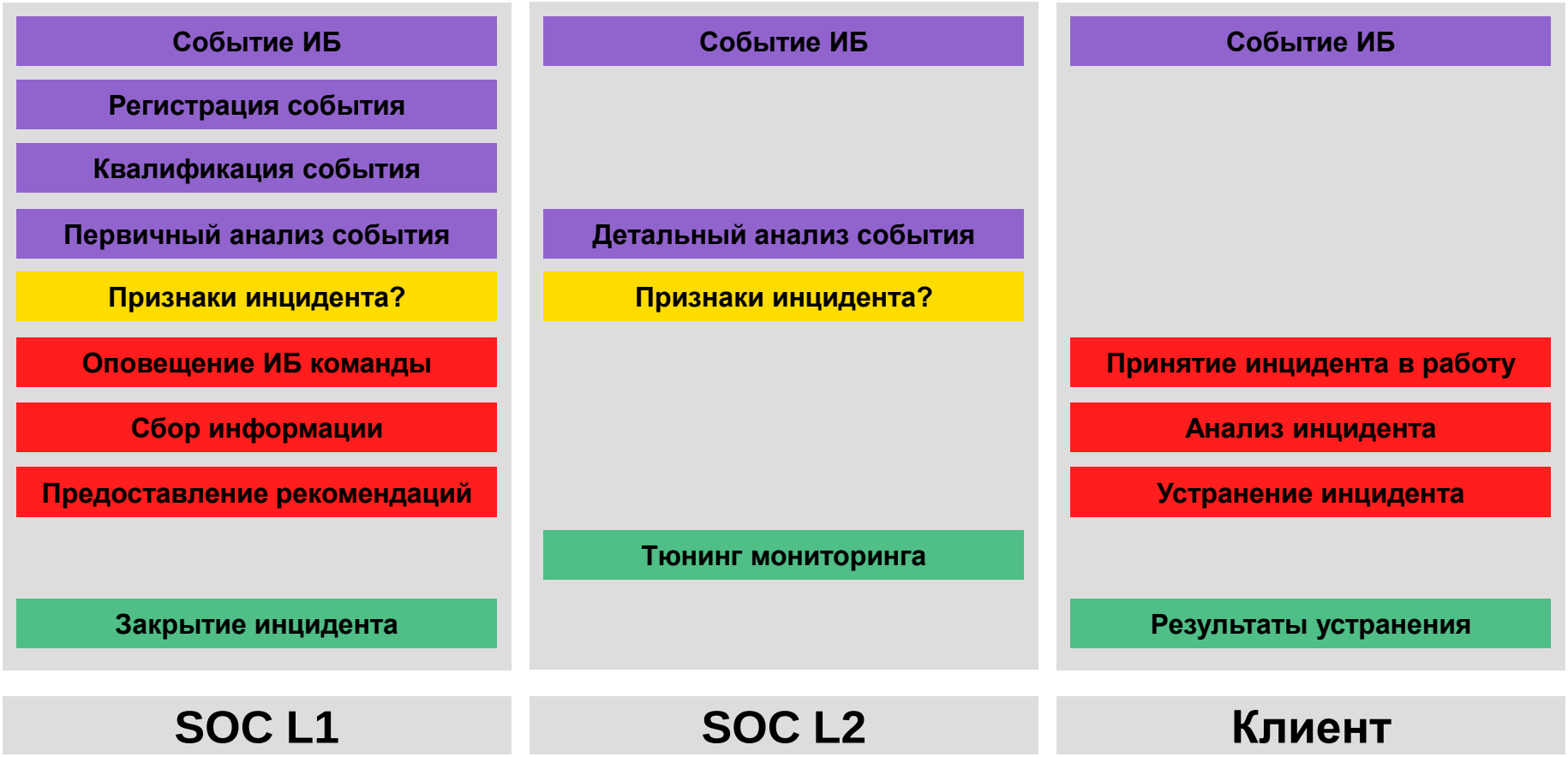
Run

- Работа с use-cases переданными в эксплуатацию
- Уведомление об инцидентах

Столько может длиться пилот



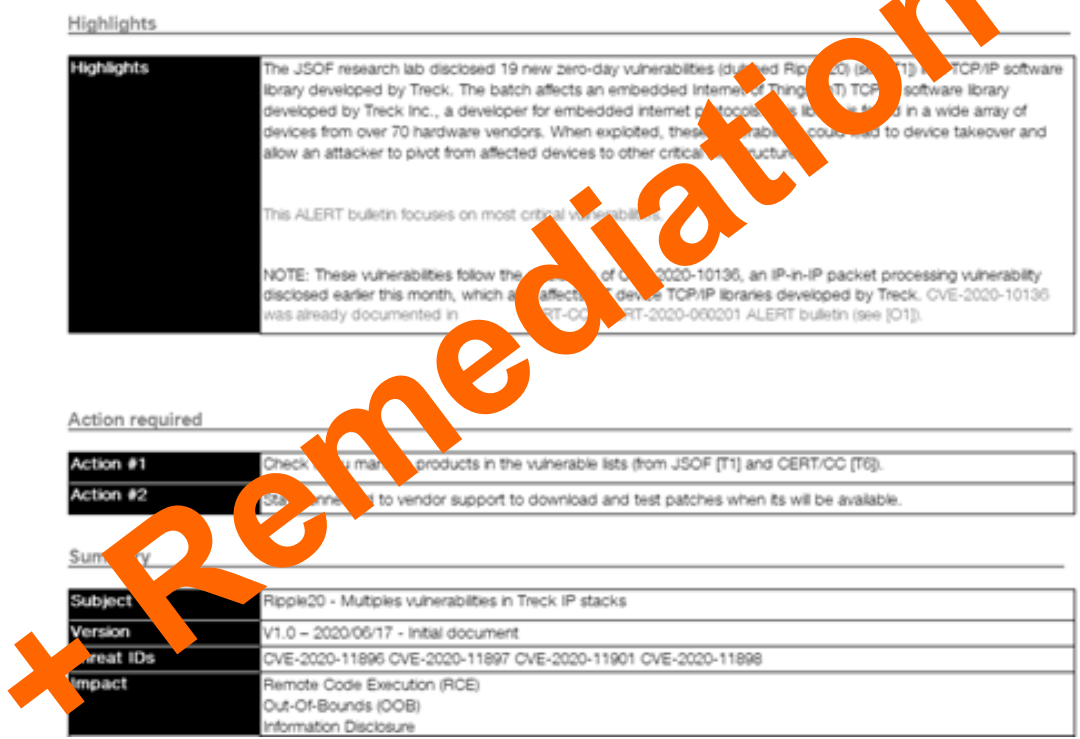
Процесс работы над инцидентами



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	

Internal CERT



Highlights

Highlights	The JSOF research lab disclosed 19 new zero-day vulnerabilities (dubbed Ripple20) (see [T1]) in a TCP/IP software library developed by Treck. The batch affects an embedded Internet of Things (IoT) TCP/IP software library developed by Treck Inc., a developer for embedded internet protocols libraries found in a wide array of devices from over 70 hardware vendors. When exploited, these vulnerabilities could lead to device takeover and allow an attacker to pivot from affected devices to other critical infrastructure. This ALERT bulletin focuses on most critical vulnerabilities. NOTE: These vulnerabilities follow the disclosure of CVE-2020-10136, an IP-in-IP packet processing vulnerability disclosed earlier this month, which also affected the Treck TCP/IP libraries developed by Treck. CVE-2020-10136 was already documented in CERT/CC VRT-2020-060201 ALERT bulletin (see [O1]).

Action required

Action #1	Check if you manage products in the vulnerable lists (from JSOF [T1] and CERT/CC [T6]).
Action #2	Stay connected to vendor support to download and test patches when its will be available.

Summary

Subject	Ripple20 - Multiples vulnerabilities in Treck IP stacks
Version	V1.0 – 2020/06/17 - Initial document
Threat IDs	CVE-2020-11896 CVE-2020-11897 CVE-2020-11901 CVE-2020-11898
Impact	Remote Code Execution (RCE) Out-Of-Bounds (OOB) Information Disclosure

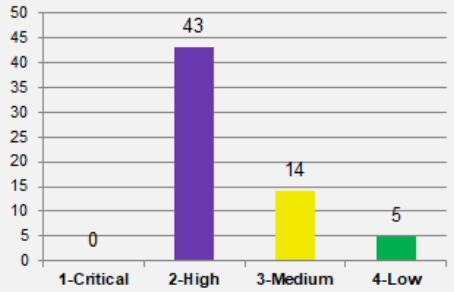
+ Remediation

Отчетность

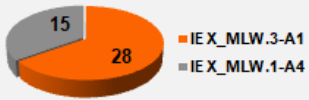
62
инцидентов

42
дополнительных отчета работе средств АВЗ

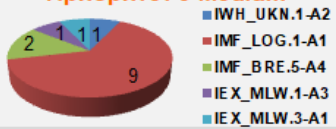
Распределение инцидентов по приоритетам



Приоритет 2-High



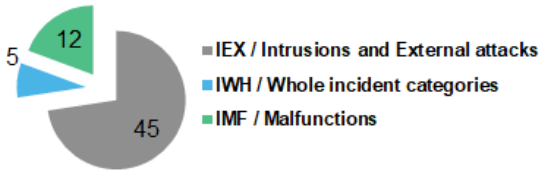
Приоритет 3-Medium



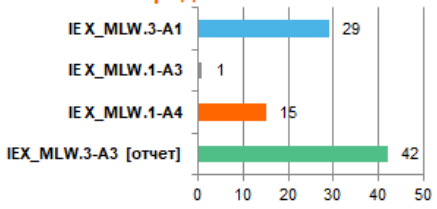
Приоритет 4-Low

IEX_MLW.3-A1 – Обнаружение вредоносного ПО по сообщениям АВЗ
IEX_MLW.1-A4 – Обнаружение вредоносного ПО по сетевыми IoC (например, взаимодействие с C&C)
IEX_MLW.1-A3 – Выявление массового заражения
IWH_UKN.1-A2 -- Выявление обращений к контролируемым объектам в нелегитимное время (не более 2 объектов, которые утверждаются при старте пилота) (Для Windows, Unix)
IMF_LOG.1-A1 – Остановка передачи событий от настроенных источников (в течение 1/24 часов)
IMF_BRE.5-A4 -- Выявление несанкционированных отключений средств АВЗ на контролируемых узлах/KSC Антивирусные базы устарели
IMF_BRE.5-A5 -- Выявление несанкционированных отключений средств АВЗ на контролируемых узлах/KSC Антивирусная защита отключена
IEX_MLW.3-A3– [отчет о срабатываниях АВЗ] выявление антивирусом сигнатур, входящих в список угроз высокой критичности

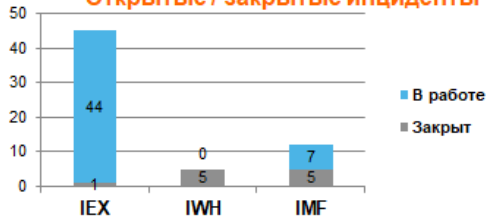
Распределение атак по категориям



Вредоносное ПО



Открытые / закрытые инциденты



Функций много…

Колл-центр	Мониторинг и приоритезация событий	Координация деятельности по реагированию	Удаленное реагирование на инциденты
Реагирование на инциденты с выездом на объект	Анализ инцидентов	Анализ угроз	Анализ вредоносного ПО и НДВ
Разработка сценариев реагирования	Разработка правил корреляции	Разработка инструментария	Реализация мер защиты
Контроль периметра сети	Управление средствами защиты периметра	Управление инфраструктурой SOC	Настройка и обслуживание сенсоров
Выявление и анализ уязвимостей	Сбор и анализ бюллетеней безопасности	Подготовка бюллетеней безопасности	Публикация бюллетеней безопасности
Тестирование на проникновение	Оценка технических решений	Консультирование по вопросам ИБ	Forensic/Расследование инцидентов
Расследование действий инсайдеров	Повышение осведомлённости	Распространение знаний о способах проведения атак	Распространение знаний о способах противодействия атакам

Функций много… как можно делать всё

Колл-центр	Мониторинг и приоритезация событий	Координация деятельности по реагированию	Удаленное реагирование на инциденты
Реагирование на инциденты с выездом на объект	Анализ инцидентов	Анализ угроз	Анализ вредоносного ПО и НДВ
Разработка сценариев реагирования	Разработка правил корреляции	Разработка инструментария	Реализация мер защиты
Контроль периметра сети	Управление средствами защиты периметра	Управление инфраструктурой SOC	Настройка и обслуживание сенсоров
Выявление и анализ уязвимостей	Сбор и анализ бюллетеней безопасности	Подготовка бюллетеней безопасности	Публикация бюллетеней безопасности
Тестирование на проникновение	Оценка технических решений	Консультирование по вопросам ИБ	Forensic Расследование инцидентов
Расследование действий инсайдеров	Повышение осведомлённости	Распространение знаний о способах проведения атак	Распространение знаний о способах противодействия атакам

Orange Russia

Orange Cyberdefense

Партнеры

Процессы в SOC: советы и заблуждения

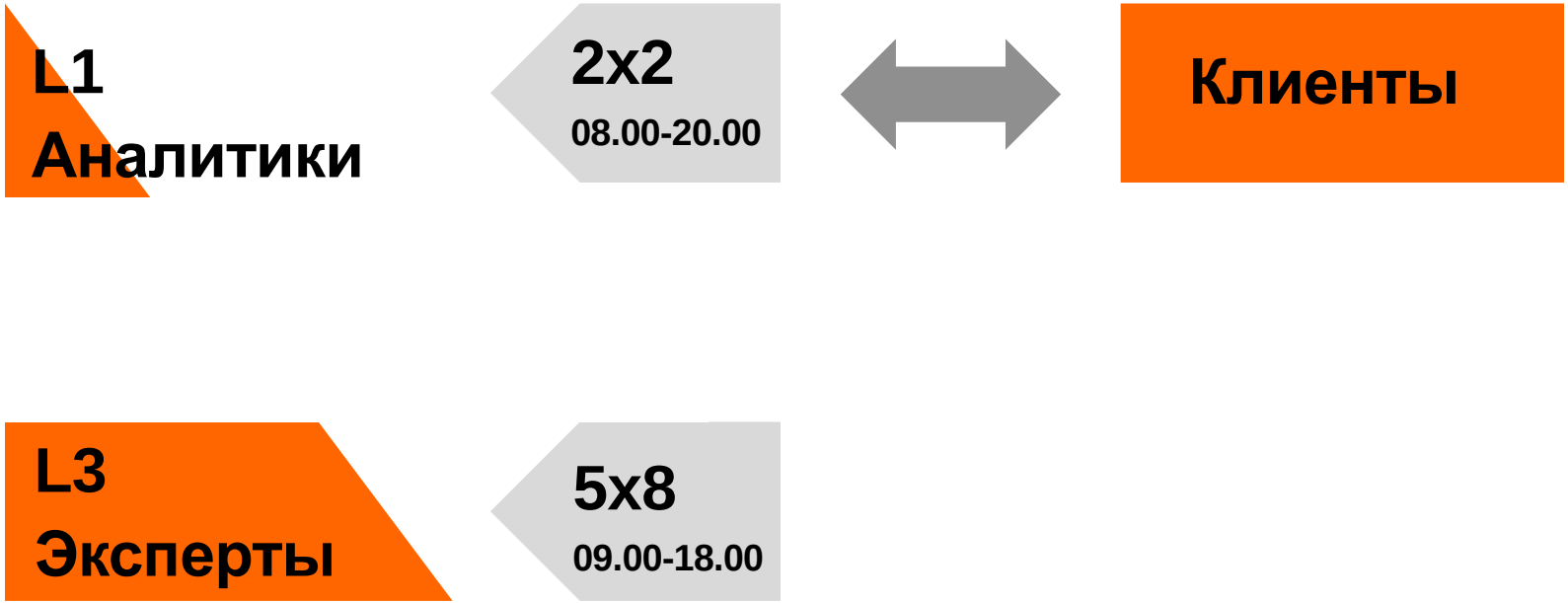
- Единые процессы взаимодействия внешнего и внутреннего SOC
- Периодическое сканирование с контролем исполнения в SOC
- Разделяйте аналитику и обслуживание

- Можно не реагировать на оповещения SOC
- Политику обработки инцидентов можно не вводить

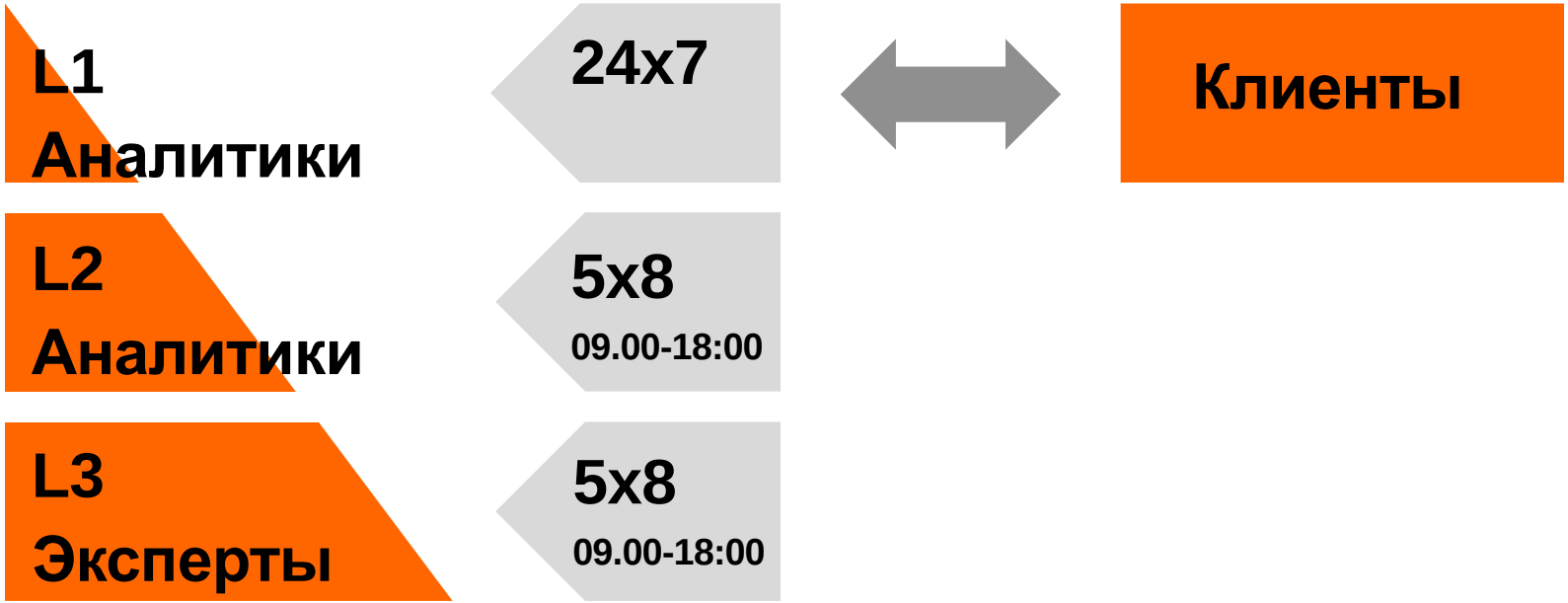
- Разделите зоны ответственности между клиентом и SOC
- Договоритесь о сроках пилота
- Внедрите сроки обратной связи

Команда SOC

Команда Internet Umbrella



Core команда SOC



Кто чем занимается?

L1 Аналитики		**Работа с инцидентами в IR** **Составление отчетов** **Взаимодействие с клиентами по инцидентам**
L2 Аналитики		**Работа с инцидентами в IR** **Проведение углубленного анализа инцидентов**
L3 Аналитики	**Pentesters** **Solution experts** **Technical architects** **Security experts**	**Разработка use cases, настройка включений** **Аудиты/тесты на защищенность** **Имплементация новых функций**
Группа реагирования	**Security team** **IT team**	**Оперативное реагирование** **Устранение инцидентов** **Координация действий при инциденте**

Кто чем занимается?

Группа эксплуатации	Admins (network, cloud, infrastructure platforms,	Поддержка инфраструктуры Взаимодействие с вендорами Поддержка платформ виртуализации IaaS Планирование MW & patch management
Проектная группа	PM Professional services SM SOC team	Ведение PoCs Обсуждение текущих активностей с клиентами Доработка новых функций услуги Отчетность и взаимодействие с руководством
Консалтинг	Professional services Presales Technical architect	Проработка управляемых ИБ сервисов и аутсорсинга для клиентов Организация пилотов и PoC Разработка проекта под клиента
R&D	Professional services Technical architect Solution experts	Разработка сценариев детектирования и реагирования Реализация средств автоматизации Внедрение новых функций

Клиент
внешний/внутренний

Группа реагирования

ИБ менеджер
ИБ руководитель

инциденты

отчеты и улучшения

Кто с кем взаимодействует?

L1

ИБ Менеджер

L2

L3

Orange SOC

Минимальный состав SOC

L1 Аналитики — 5 сотрудников

L2 Аналитики — 2 сотрудника

L3 Аналитики

Группа реагирования (внутренний SOC)

Консалтинг

Проектная группа

Группа обслуживания

External partner skill center

Команда SOC: советы и заблуждения

- Стремиться нужно к выделенному центру
- Профильное образование команды
- Одна IRP
- Обучение смежным направлениям

- Построить команду не занимает много времени
- Можно начать с Fast start и собрать неполную команду, потом добрать людей
- У команды много свободного времени, можно добавить других функций

- Введите дежурство L2 экспертов на постоянной основе
- Введите процесс передачи смены
- Во внутреннем SOC можно и нужно вводить сроки обратной связи
- Для проектной части используйте Agile-методологии

Спасибо!

#StaySafe

Юрий Бармотин
yury.barmotin@orange.com

orange™ Business Services