

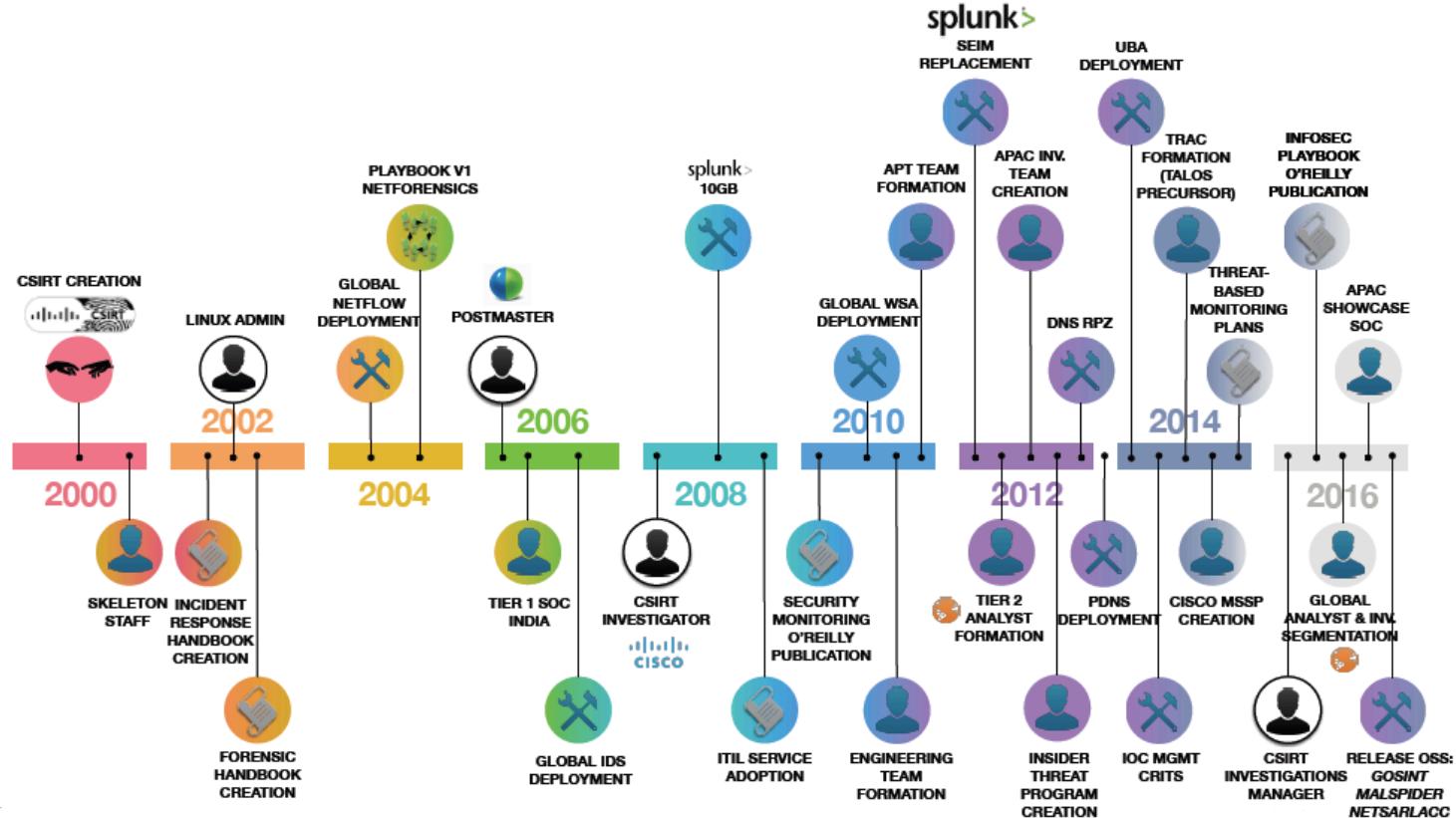
# От SOC v0.1 к SOC v2.0: от простого к инновационному

Алексей Лукацкий

Бизнес-консультант по кибербезопасности

31 мая 2019

# Внутри Cisco SOC строится уже 19 лет!



# Выбросьте триаду на помойку



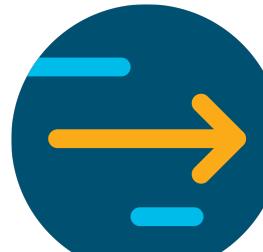
Стратегия



Миссия / цели



Команда



Процессы



Окружение



Технологии



Intelligence

# Начиная с SOC v0.1

Вы только мониторите или также реагируете?



# Команда NG SOC

<b>Ядро SOC</b>	<b>CSIRT</b>	<b>CTA/CTI</b>	<b>Engineering</b>
<ul style="list-style-type: none"><li>Аналитики</li><li>Investigator</li><li>1<sup>st</sup> Responder</li><li>SIEM/NTA/EDR/UEBA</li><li>SOC Lead</li></ul>	<ul style="list-style-type: none"><li>Incident Handler</li><li>Incident Responder</li><li>Forensic Expert</li></ul>	<ul style="list-style-type: none"><li>Data Scientist</li><li>Hunters</li><li>Threat Intelligence</li></ul>	<ul style="list-style-type: none"><li>Архитектор SOC</li><li>Специалист по Use Cases (правилам)</li><li>Программисты</li></ul>
<b>SME</b>	<b>Поддержка</b>	<b>AVMT</b>	
<ul style="list-style-type: none"><li>... по продуктам</li><li>... по SIEM</li><li>... по уязвимостям</li><li>... по compliance</li></ul>	<ul style="list-style-type: none"><li>Контроль качества</li><li>Администратор SOC</li><li>Безопасность</li></ul>	<ul style="list-style-type: none"><li>Сканирование сети</li><li>Тестирование приложений</li><li>Red Team</li></ul>	
<ul style="list-style-type: none"><li>Управление средствами ИБ</li></ul>			

# Какой SOC вы хотите?

Мода SOC v0.1	Compliance SOC v0.5	Бизнес SOC v1.0+
<ul style="list-style-type: none"><li>• SIEM – ядро SOC</li><li>• SOC нужен для ГосСОПКИ</li><li>• У всех есть и мне нужен</li></ul>	<ul style="list-style-type: none"><li>• Ориентация на НПА ЦБ / ФСБ / ФСТЭК</li><li>• «Заблокировал и забыл»</li><li>• Нет Use Case и Playbook</li><li>• Отсутствие интеграции с ИТ и бизнесом</li><li>• Отсутствие процессов</li></ul>	<ul style="list-style-type: none"><li>• Ориентация на инциденты, а не события</li><li>• Защита критичных активов</li><li>• Ориентация на людей и процессы в SOC, а не технологии</li><li>• ИБ с точки зрения бизнеса</li><li>• Контроль качества</li></ul>

# Что вы будете охватывать вашим SOCом?



Любые  
пользователи

- Сотрудники
- Контрактники
- Партнеры



Любые  
устройства

- Корпоративные
- Собственные
- IoT



Любые  
приложения

- ЦОД
- Мультиблако
- SaaS



В любых  
местах

- Внутри сети
- Через VPN
- Вне сети

# SOC: сервисы vs процессы

## Сервис

- Управление значимыми результатами деятельности, без погружения в детали реализации
- Поставщик отвечает за результат, а потребитель – за корректные требования к результату

## Процесс

- Непосредственное управление деятельностью
- За конечный результат отвечает потребитель, устанавливающий правила для процессов

# Сервисная стратегия SOC

Видение стратегии	Драйвера, ожидания заказчика, ключевые принципы и ожидаемый результат
Резюме по сервисам	Описание сервисов SOC – модель реализации, владелец, вход и выход для сервиса, компоненты
Ключевые процессы	Описание ключевых процессов, необходимых для реализации сервисов SOC
Организационная стратегия	Описание структуры команды SOC и всех ролей
Технологическая стратегия	Описание технологического стека SOC

Вы думаете о  
SOC? А у вас  
есть, что  
мониторить?

# Сначала внедрите то, что вы хотите мониторить



Прежде чем строить SOC или отдавать мониторинг на аутсорсинг в внешний SOC, сначала внедрите то, что будет отдавать данные



Для мониторинга МСЭ на периметре и антивируса на ПК SOC не нужен!



## ВНИМАНИЕ

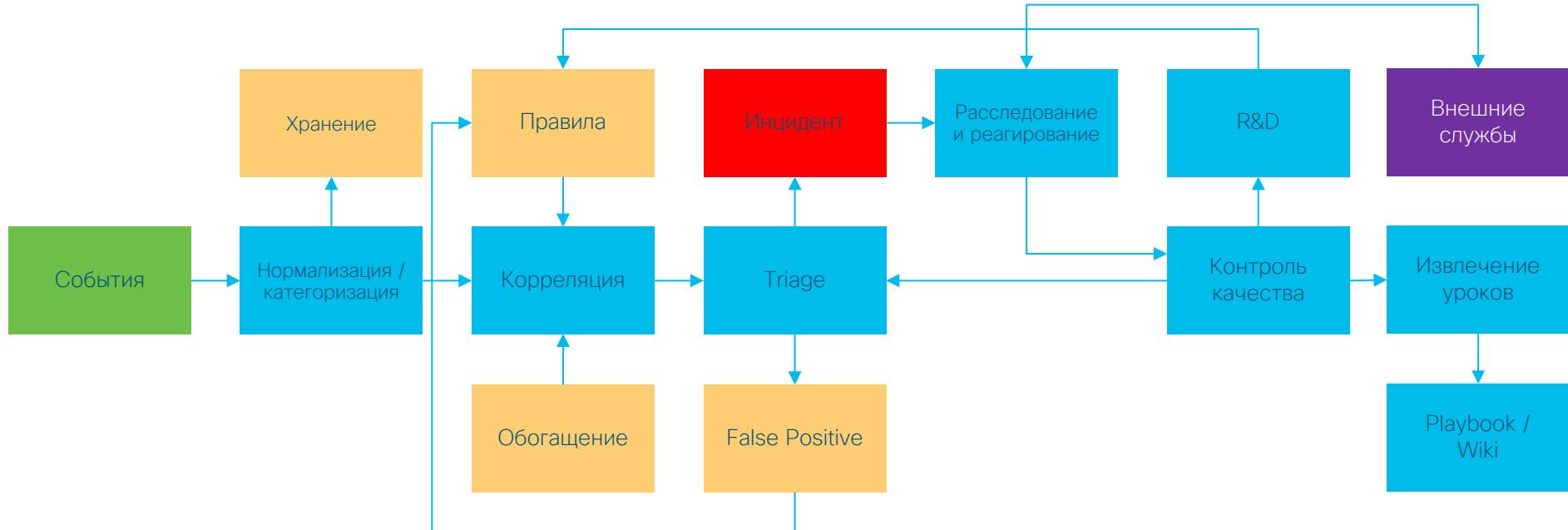
Это частый запрос в наш аутсорсинговый SOC



# Какие данные собирает ваш SOC?

События ИБ	Сетевые события	Приложения и устройства	ИТ-инфраструктура
<ul style="list-style-type: none"><li>· МСЭ</li><li>· IDS</li><li>· AV / EPP / EDR</li><li>· DLP</li><li>· VPN</li><li>· Web-доступ</li><li>· Обманные системы</li><li>· WAF</li></ul>	<ul style="list-style-type: none"><li>· Маршрутизаторы</li><li>· Коммутаторы</li><li>· Точки доступа</li><li>· DNS-сервера</li><li>· Частные облака</li><li>· Публичные облака</li></ul>	<ul style="list-style-type: none"><li>· Базы данных</li><li>· Сервера приложений</li><li>· Web-приложения</li><li>· SaaS-приложения</li><li>· Мобильные устройства</li><li>· Десктопы и лэптопы</li></ul>	<ul style="list-style-type: none"><li>· Конфигурации</li><li>· Геолокация</li><li>· Владельцы</li><li>· Инвентаризация</li><li>· Сетевые карты</li><li>· Уязвимости</li></ul>

# Продукты ⇒ Security Operations ⇒ SOC



Security Operations объединяет множество решений в единый комплекс!

платных и бесплатных

Учитываете ли вы  
физиологию или  
когда вы поймете,  
что L1 вам не  
нужна?

# Сейчас вы увидите видео

Посчитайте  
количество передач  
мяча, сделанных  
людьми в белых  
футболках!





Правильный  
ответ – 16



Вы заметили  
гориллу?



Вы заметили  
уход девушки  
в черной  
футболке?!



Вы заметили  
смену цвета  
штор на  
заднем  
плане?!



# Вы учитываете физиологию работы аналитика?



После 12-ти минут непрерывного мониторинга аналитик пропускает 45% активности на мониторе. После 22-х – 95%



После 20-40 минут активного мониторинга у аналитика наступает психологическая слепота



Подумайте о ротации смен, режиме отдыха аналитиков и, возможно, замене L1 машинным обучением или иными технологиями



# Почему первая линия SOC не нужна



Аналитики L1 занимаются мониторингом событий и обнаружением простых инцидентов, а также открытием заявок



Автоматизация поможет исключить аналитиков L1, которые и так видят около 10% всего того, что должны



Оставшиеся 90% – это игра и в нее надо быть вовлеченным



Уровень  
ротации  
аналитиков L1  
– около 90%

# Что ищут аналитики L1 – известное или неизвестное?

## Базовый уровень

- Security Device Management
- Collective Security Intelligence
- Log Collection
- Event Correlation
- Rule-Based Analytics



Speed



Accuracy



Focus

## Средний уровень

- + Deeper Investigation Toolkit
- + Statistical Anomaly Detection
- + NetFlow Generation
- + Protocol Metadata Extraction
- + Data Enrichment



Speed



Accuracy



Focus

## Продвинутый

- + Real-time Visual Analytics
- + Machine Learning (Supervised and Unsupervised)
- + Raw Capture
- + Proactive Threat Hunting
- + Advanced Statistical Analytics (polymorphic)



Speed



Accuracy



Focus

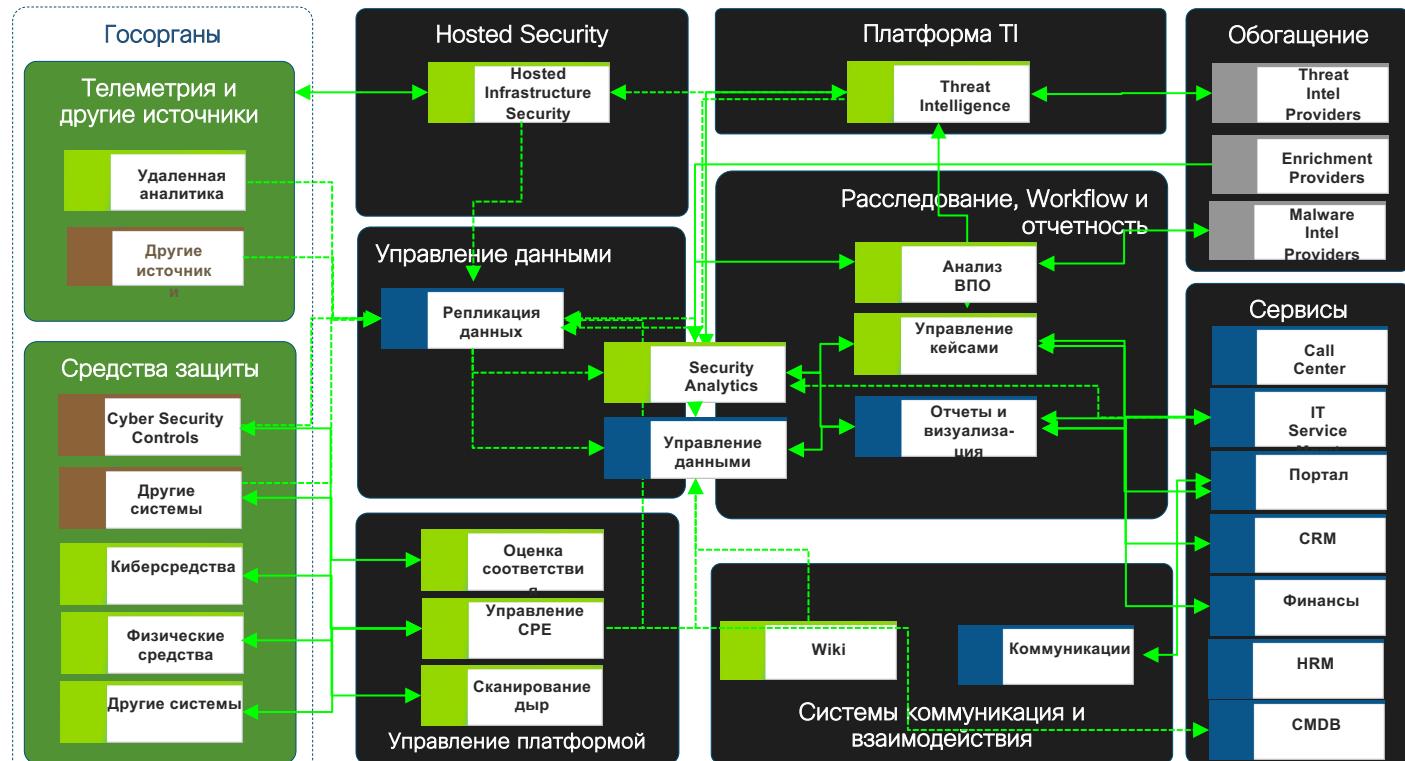
L1 – это для этого уровня зрелости аналитических технологий SOC

SOC v2.0  
базируется не на  
SIEM

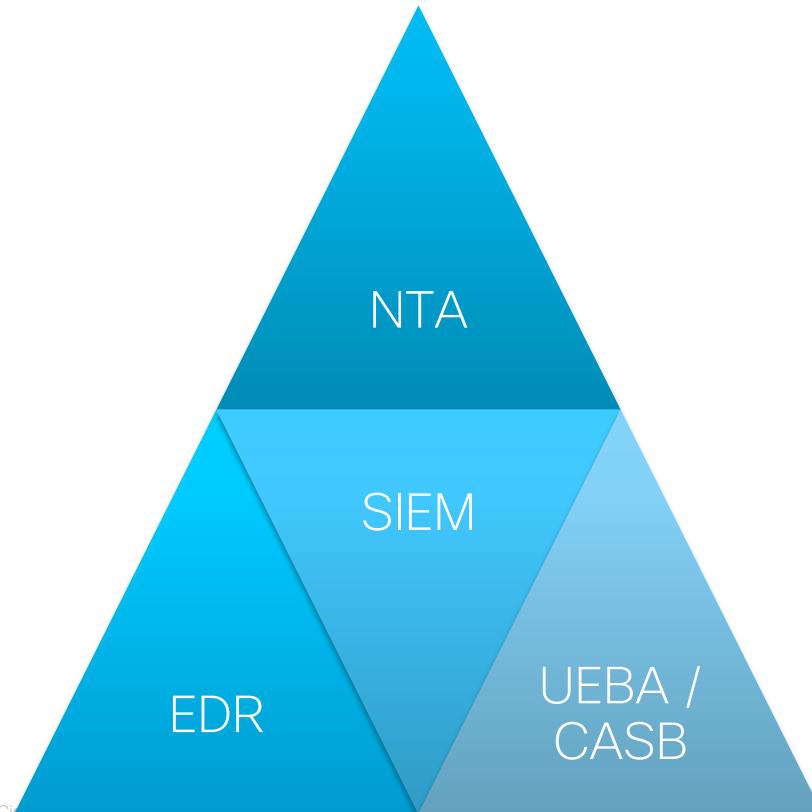
# В чем разница?

Возможности	Традиционный SOC	SOC нового поколения
<ul style="list-style-type: none"><li>• Обнаружение угроз</li><li>• Классификация угроз</li><li>• Анализ инцидентов и составление плана реагирования</li><li>• Локализация угрозы</li><li>• Восстановление от угрозы</li><li>• Время на возврат к исходному состоянию</li></ul>	<ul style="list-style-type: none"><li>• В среднем 150 дней</li><li>• В течение часов</li><li>• В течение дней</li></ul> <ul style="list-style-type: none"><li>• В течение часов</li><li>• В течение дней</li><li>• В течение недель</li></ul>	<ul style="list-style-type: none"><li>• Непрерывно</li><li>• В реальном времени</li><li>• Менее часа</li></ul> <ul style="list-style-type: none"><li>• За минуты</li><li>• В течение часов</li><li>• В течение дней</li></ul>

# Архитектура современного SOC

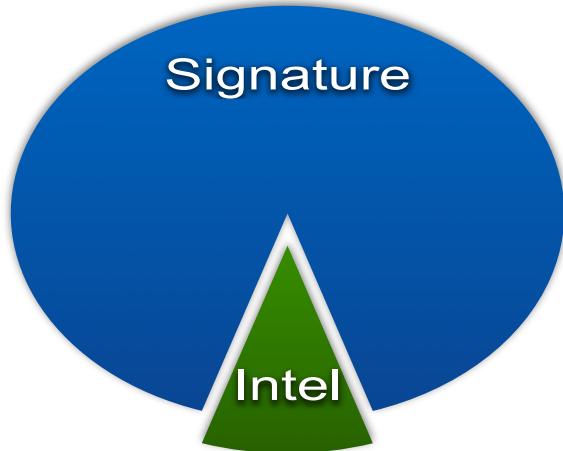


# Security Analytics Suite

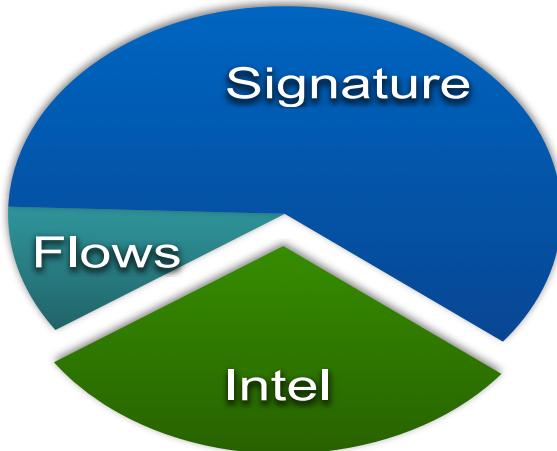


# Cisco SOC: раньше и сейчас

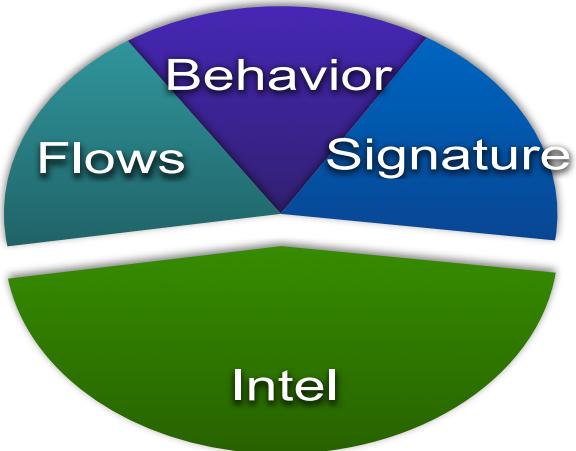
В прошлом



2012



2013+



Не только  
технологии и  
автоматизация

Workflow для отслеживания утекших паролей

# Конфиденциальная иллюстрация

# Мониторинг Darknet для отслеживания утекших паролей

## Проблема

- Учетные записи сотрудников появляются в онлайн-дампах
- С хешами паролей или в открытом виде
- Утечки данных с скомпрометированных внешних сайтов
- Корпоративные адреса использовались при регистрации
- Опасность в использовании паролей для других сервисов

## Действия

- Использование специализированных сервисов
  - <https://haveibeenpwned.com/>
  - <https://breachalarm.com/>
  - <https://www.infoarmor.com/>
- Уведомление сотрудников напрямую и через скомпрометированных провайдеров услуг
- Автоматический workflow для уведомления сотрудников

# Мониторинг Darknet для отслеживания утекших паролей

The screenshot shows an email message in a Microsoft Outlook-style interface. The subject of the email is "Notice of external account / password compromise - Inbox". The message is from "noreply@cisco.com <no-reply@cisco.com>" on Monday, 8 May 2017 at 13:03, to "Alexey Lukatsky (alukatsk)". The message content is as follows:

Hello Alexey,

This is a notification from the Cisco Computer Security Incident Response Team (CSIRT).

We have been notified that a service using [alukatsk@cisco.com](mailto:alukatsk@cisco.com) email address and UNKNOWN password may have been compromised. The account information was obtained by monitoring the Internet and other sources. Because of the source and scope, the validity of these credentials cannot be easily verified. We do not know the website this leak occurred on, only that your credentials have been made available online.

Please take immediate action to update your password on any site where your [alukatsk@cisco.com](mailto:alukatsk@cisco.com) email address was used. The following accounts could be affected:

- Cisco (CEC, email, etc.)
- Email (Gmail, Yahoo! Mail, etc.)
- Financial (bank, 401k, etc.)
- Social media (Twitter, Facebook, etc.)
- Services (Internet, phone, cable, etc.)
- E-commerce (eBay, Amazon, PayPal, etc.)

If you have questions regarding this email, refer to the following FAQs: <https://cisco.jiveon.com/docs/DOC-1400312>. If you are unable to find an answer to your question, please contact us at [cisirt-ext-comms@cisco.com](mailto:cisirt-ext-comms@cisco.com).

Please remain vigilant and do not click on or respond to emails that request personal data or look suspicious. You can confirm the validity of this email, and ensure that any links are safe to click, by visiting the Cisco Information Security PhishPond site: <http://phishpond.cisco.com/>.

Regards,  
CSIRT

About CSIRT:  
<http://wwwin.cisco.com/c/cec/organizations/security-trust/infosec/teams/csirt.html>

# Нам разрешили ходить в шортах 😊

Announcement: Dress Code

• Company News <[news@securefileshares.com](mailto:news@securefileshares.com)>  
• Alexey Lukatsky (alukatsk)

Tuesday, 28 May 2019 at 15:55  
[Show Details](#)



Hi Team,

A friendly reminder that all Cisco Systems employees must follow the Dress Code policy. Each region sets its own rules and guidelines so it important to make sure we are all showing up in appropriate attire.

Please see the the dress code standard for your regions.

[\*\*Corp Dress Code\*\*](#)

This email may contain confidential and privileged information for the sole use of the intended recipient. If you are not the intended recipient, please contact the sender and delete all copies. Any review or distribution by others is strictly prohibited. Thank you.

Не все можно  
купить за деньги –  
посмотрите в  
сторону open  
source

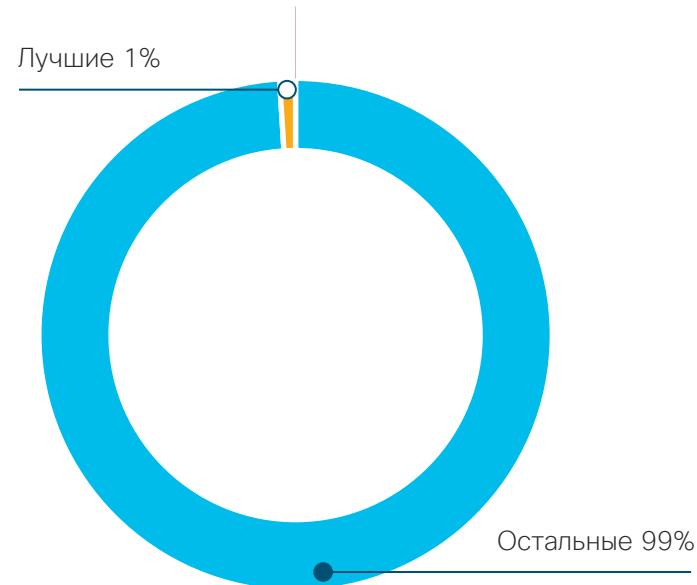
# Покупать или создавать инструментарий?



99% SOСов используют готовые, приобретенные решения по ИБ



1% SOСов разрабатывают свой инструментарий или дорабатывают open source решения

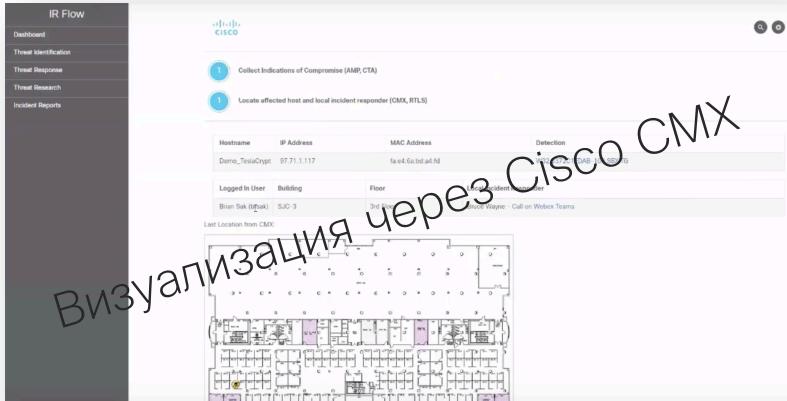


# Пример: irflow

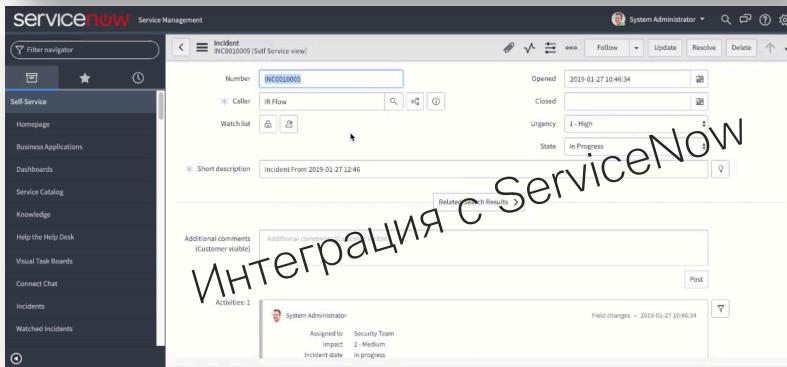
Date	Hostname	IP Address	MAC Address	Detection
2019-01-20T18:17:41+00:00	Demo_TeslaCrypt	97.71.1.117	fa:e8:6e:bd:a4:fd	W32.3372C1EDAB-100.SBX.TG
2019-01-20T19:10:59+00:00	Demo_TDSS	205.186.185.220	bb:74:4b:8f:ea:8d	Eldorado:Alureon-tpd
2019-01-20T19:09:01+00:00	Demo_Teba	97.187.29.224	c4:f6:ab:17:86:11	W32.Variant:Teba.15hl.1201
2019-01-20T19:07:18+00:00	Demo_Dyre	210.69.253.192	28:7c:a1:fb:4e:e3	GenericKD:Dyreze-tpd
2019-01-20T19:03:17+00:00	Demo_SFECiar	110.42.99.68	4b:25:e6:10:9:ca:0	Win32.DemoMal.Rat.Client
2019-01-20T19:02:42+00:00	Demo_Zbot	240.52.74.250	17:16:cc:09:65:3a	ZBot:FakeAlert-tpd
2019-01-20T19:01:09+00:00	Demo_CozyDuke	208.68.74.158	a4:d2:61:87:32:2a	W32.GenericKD:CozyDuke.B.18f0.1201
2019-01-20T19:00:33+00:00	Demo_Ramnit	42.155.252.27	b9:d5:3f:51:5f:a2	W32.Ramnit.A
2019-01-20T19:00:19+00:00	Demo_Uptane	193.87.202.8	fe:3b:e9:1c:07:e9	Win.Trojan.Uptane.tht.VRT

- Приложение для автоматизации процесса реагирования на инциденты с помощью решений Cisco
- Интеграция различных решений Cisco и других компаний
- Исходный код выложен на GitHub

# Пример: irflow



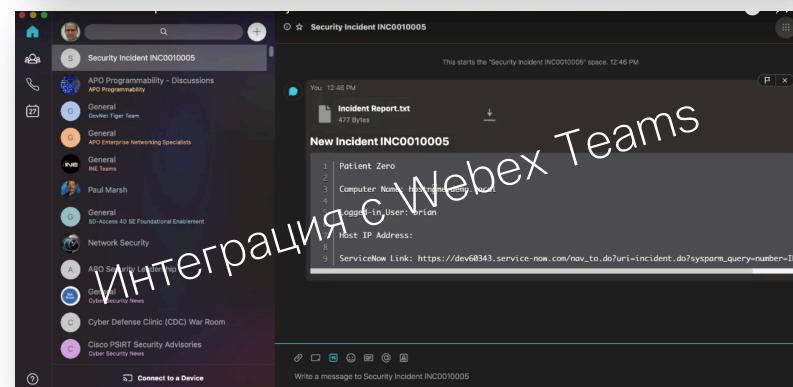
Визуализация через Cisco CMX



Интеграция с ServiceNow



Оформление тикета



Интеграция с Webex Teams

Продумайте  
варианты оценки  
эффективности

# Разработка Dashboard для разных задач

## CSIRT WEEKLY ANALYTICS

Week 43(2015)  
DATE REPORTING FOR THE WEEK OF Oct 22 - Oct 28

**CASE COUNT**

High Severity Normal Severity	3 174	<b>177</b>	-14%
High Severity Normal Severity	2 48	<b>50</b>	-29%
High Severity Normal Severity	3 1,252	<b>1,255</b>	+11%

**New Cases this Week**

**Cases Closed this Week**

**Total Current Open Cases**

*Note: Difference in percentage is in comparison with last week.*

**NEW CASES BY CATEGORY**

CAT 0: Exercise/ Network Defense Test..	1
CAT 2: Denial of Service	3
CAT 3: Malicious Code	136
CAT 4: Improper Usage	2
CAT 5: Scan / Probe	5
CAT 6: Investigation	30

**DETECTION METHOD**

CISCO	43.48%
HOME GROWN	27.83%
NON CISCO	28.70%

Firepower	-50%
Firepower	5%
IOS	-28%
Homegrown	100%
WSA	3%

**THREAT DETECTED**

CSIRT has adopted the US-CERT incident categorisation system. This means all incidents handled by the Cisco CSIRT fall under one of six categories, detailed on the US-CERT page: <https://www.us-cert.gov/government-users/reporting-requirements>. A summary of the number of cases handled during the current reporting period, together with the percentage change from the previous week, is detailed below.

**%Diff. Week/Week**

CERT Category	Total Count	% Change
CAT 0: Exercise/Network Defense Testing	1	100.0%
CAT 1: Unauthorised Access	0	100.0%
CAT 2: Denial of Service	3	100.0%
CAT 3: Malicious Code	136	-20.9%
CAT 4: Improper Usage	2	-33.3%
CAT 5: Scan / Probe	5	28.6%
CAT 6: Investigation	30	36.4%

During the current reporting period, 136 of the total incident count involved malicious code (US-CERT category 3 cases). From these, a total of 79 hosts in the desktop and lab space had confirmed infections, and they were identified and sent for remediation.

**Detect-Contain-Close (Q to D)**

Time To Detect(hours)	Mean	Median	Upper 95%	Target
TLP AMBER	22	4	100	24
TLP GREEN	175	135	222	36

**THREAT INDICATORS**

TLP AMBER	TLP GREEN
136	238

**Time To Contain(hours)**

Mean	Median	Upper 95%	Target
175	135	222	36

**% OF TOTAL INDICATORS DEPLOYED INTO SPLUNK**

TLP AMBER	TLP GREEN
82.39	100.00

**Time To Close(hours)**

Mean	Median	Upper 95%	Target
738	162	475	336

**% OF DOMAIN INDICATORS DEPLOYED INTO DNS RPZ**

TLP AMBER	TLP GREEN
21.05	1.78

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

Стоимость  
украденного  
аккаунта  
клиента в  
Darknet?!



# Вопросы?



