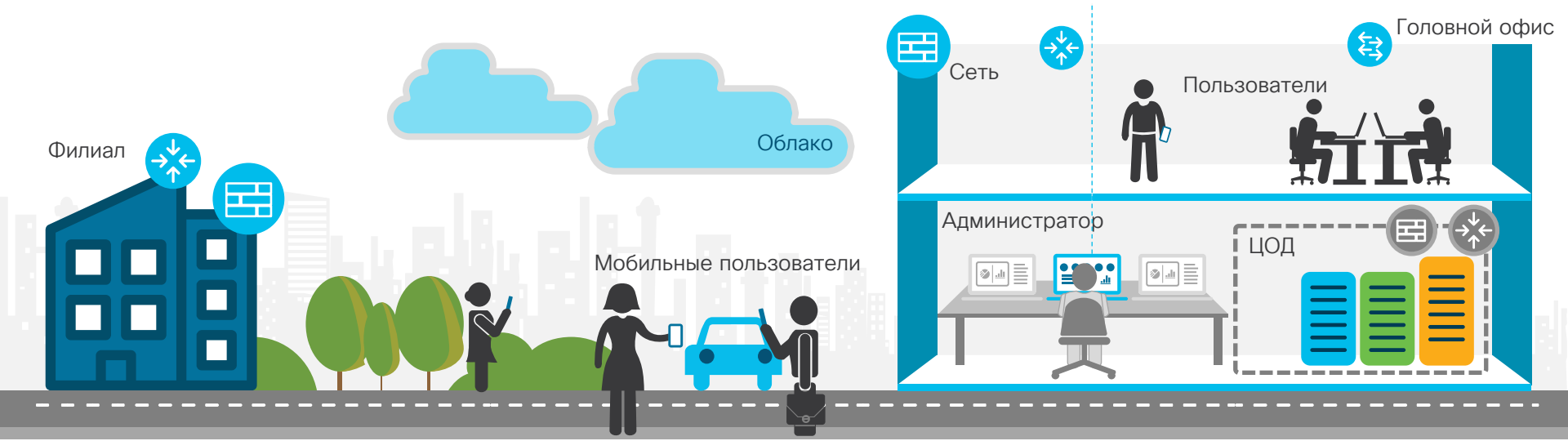
17 способов проникновения во внутреннюю сеть компании

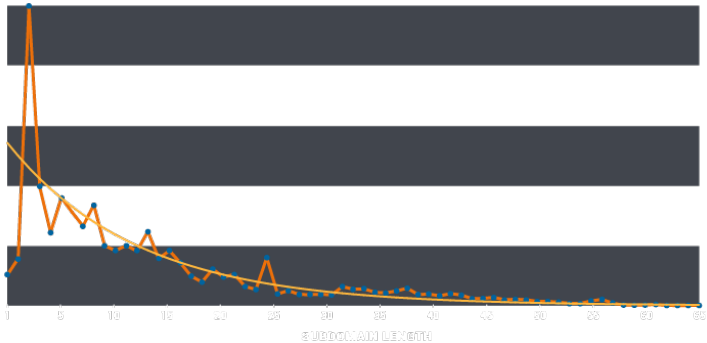
Алексей Лукацкий
Бизнес-консультант по безопасности

Посмотрите на современную, вашу, сеть

Какие варианты проникновения в нее существуют?



Утечка номеров кредитных карт через DNS



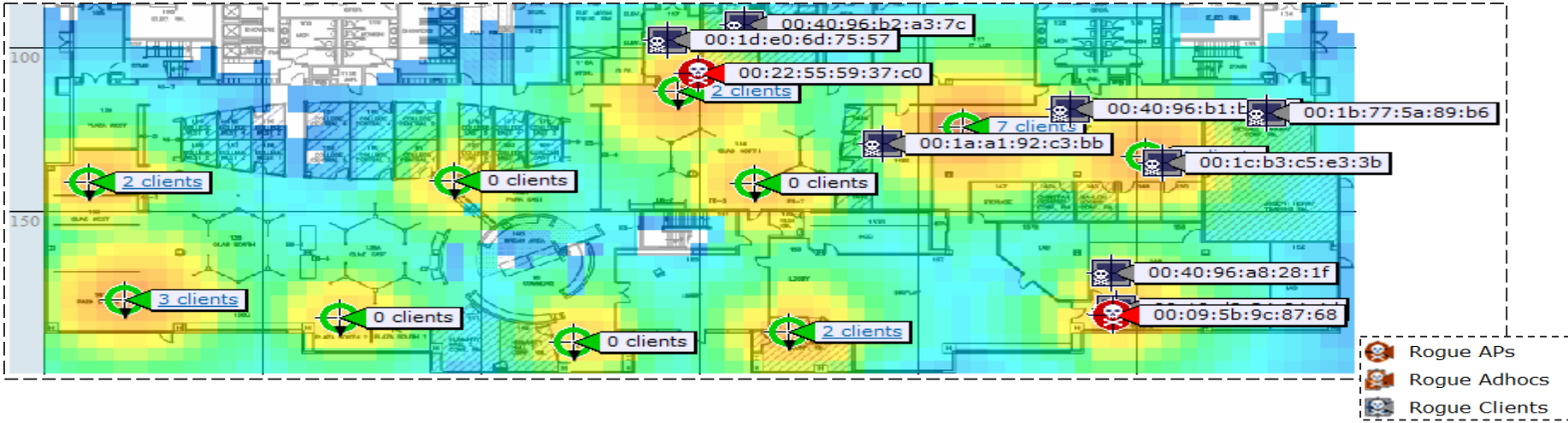
Нормальное распределение длин поддоменов

Аномалии в названии поддоменов

log.nu6timjqgq4dimbuhe.3ikfsb---отредактировано---cg3.7s3bnxqmavqy7sec.dojfgj.com
log.nu6timjqgq4dimbuhe.otlz5y---отредактировано---ivc.v55pgwcschs3cbee.dojfgj.com

Что скрывается в этой строке на 231 символ?

Взлом через Wi-Fi в контролируемой зоне



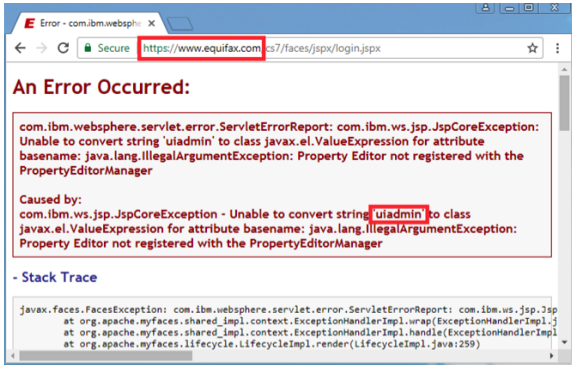
История атак на оборудование Cisco Начало 2000-х годов

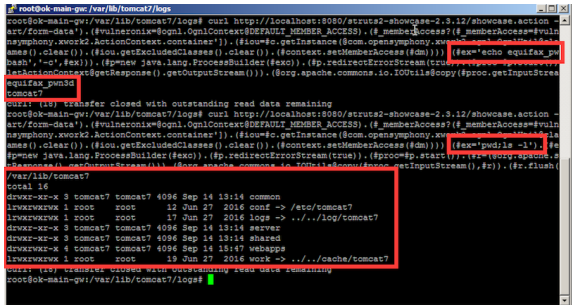
	Вариант 0	Вариант 1	Вариант 2	Вариант 3	Вариант 4	Вариант 5
Метод заражения	Статический	Статический	В процессе исполнения	В процессе исполнения	В процессе исполнения	Статический
Цель	IOS	IOS	IOS	IOS, linecards	IOS, ROMMON	IOS
Архитектура цели	MIPS	MIPS	MIPS	MIPS, PPC	MIPS	MIPS
Транспорт C&C	Неприменимо	Неприменимо	ICMP	UDP	ICMP	TCP SYN
Удаленное обнаружение	Через криптоанализ	Через криптоанализ	Используя протокол C2	Используя протокол C2	Не напрямую	Да

- Это привело к появлению множества новых технологий контроля целостности оборудования - Trust Anchor, Secure Boot, Image Signing и др.
- 44-ФЗ как угроза информационной безопасности...

Взлома Web-портала Equifax

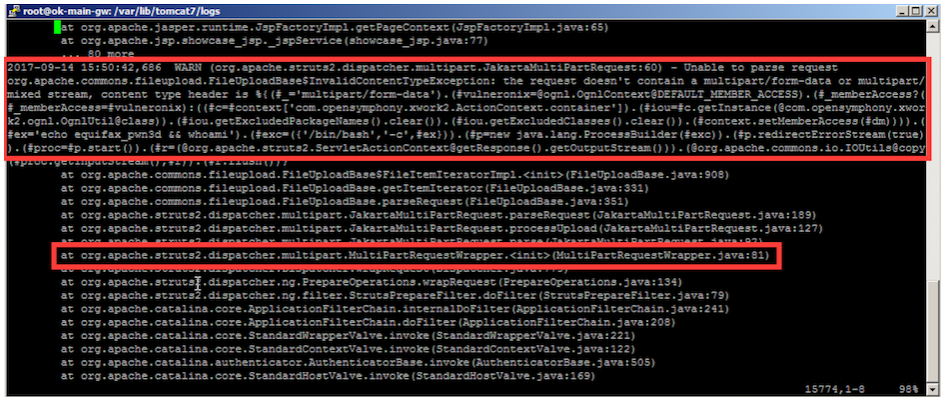
- 10 марта 2017 года злоумышленники нашли известную уязвимость на портале Equifax, позволившую получить доступ к Web-порталу и выполнять на нем команды
- Информация об уязвимости была разослана US CERT двумя днями ранее
- После идентификации уязвимости злоумышленники запустили эксплойт и получили доступ к системе, проверив возможность запуска команд
- Никаких данных украдено еще не было





Шаг 2 в атаке на Equifax: эксплуатация уязвимости

- 13 мая 2017 года злоумышленники эксплуатировали эту уязвимость и проникли во внутренние системы, выполнив ряд маскирующих процедур
- Например, использовалось существующее зашифрованное соединение для генерации запросов/получения ответов

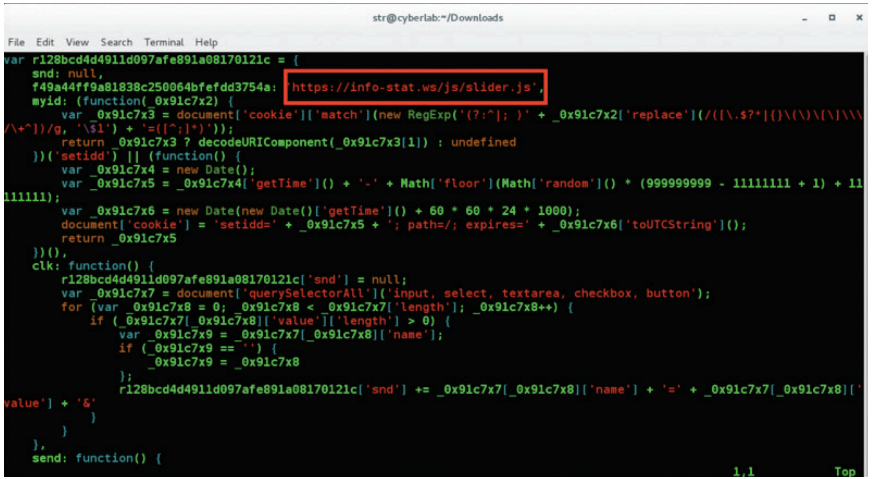


Взлом British Airways

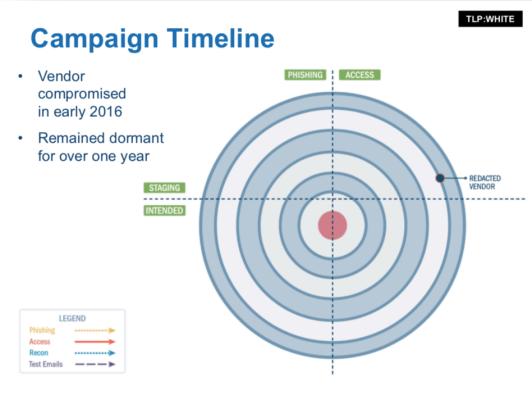
- Между 21 августа и 5 сентября 2018 года хакерская группа Magecart (или маскирующаяся под нее), взломав сервер авиакомпании British Airways, похитила данные 380 тысяч клиентов, включая их ПДн и финансовую информацию
- Позже BA сообщила, что могли пострадать еще 185 тысяч клиентов

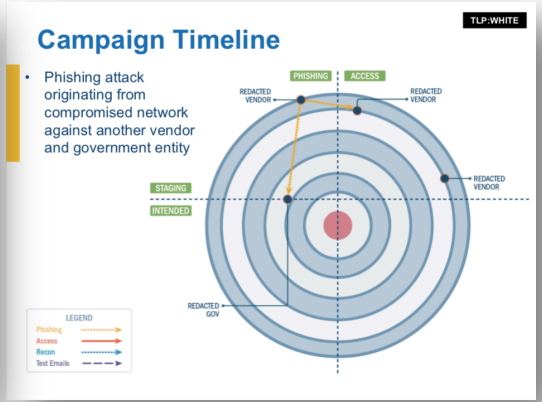
Начало сценария схоже с Equifax

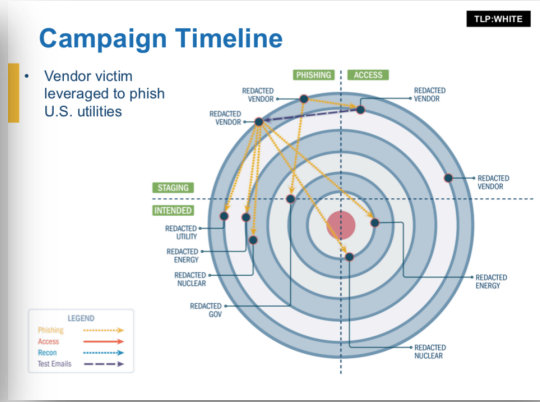
- Отличие в том, что в случае с BA был взломан сайт авиакомпании и подменен JavaScript, собирающий данные клиентов, с последующей пересылкой данных на вредоносный ресурс baways.com
- Также есть предположение, что взломан мог быть не сайт BA, а CDN, используемый провайдерами связи для кеширования популярных ресурсов или сервер третьей стороны

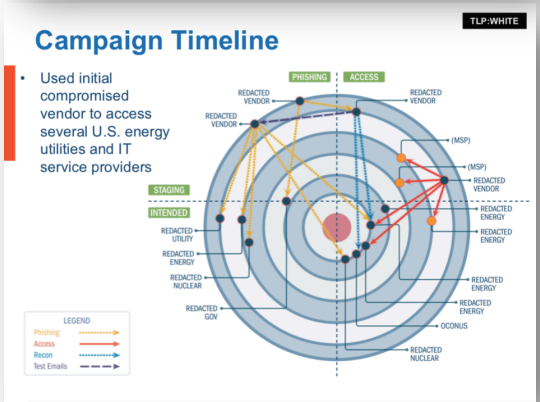


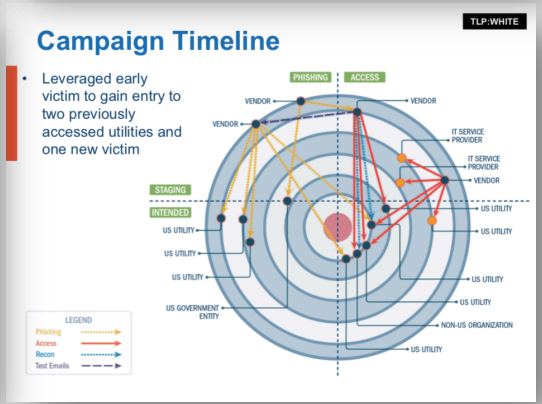
Атака «водопой» (water hole)









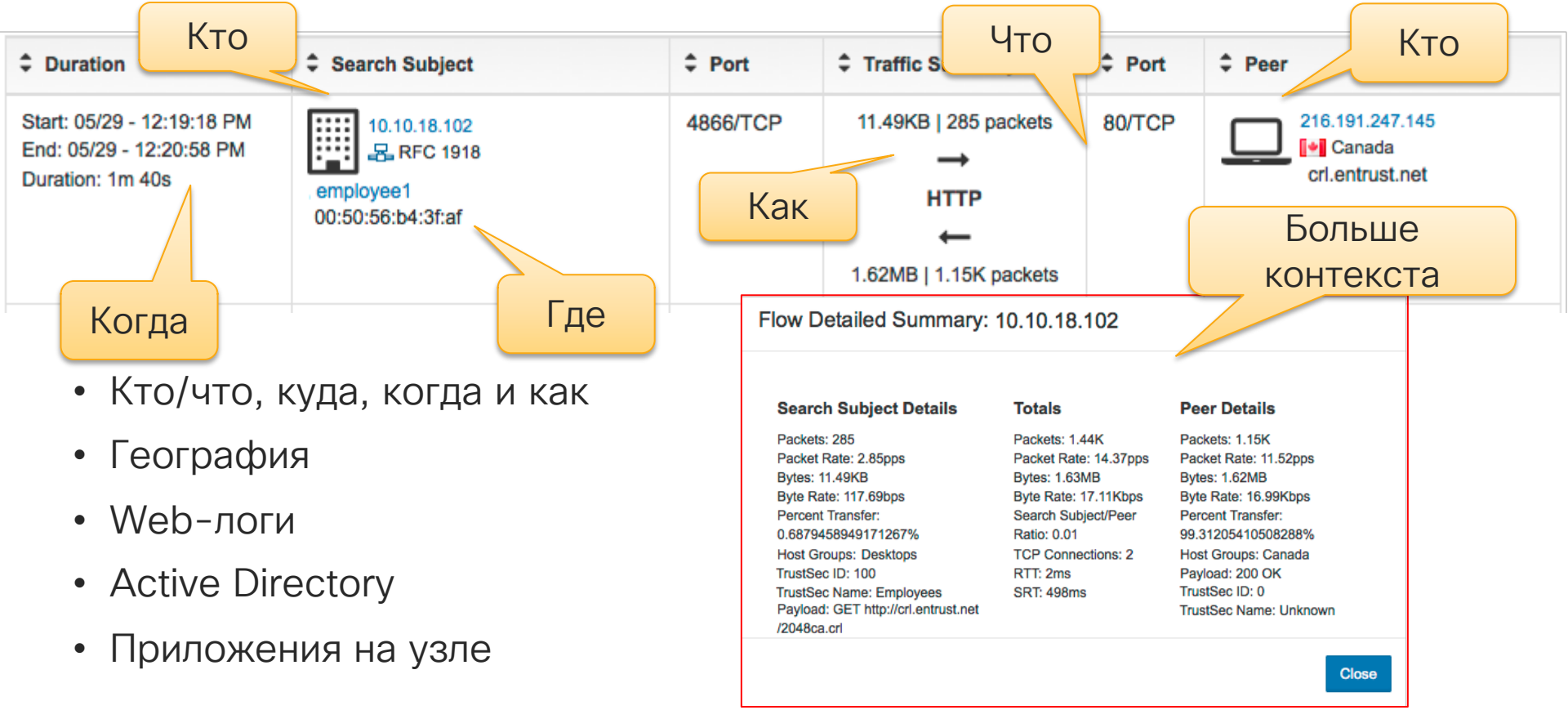


А также взлом ASUS

17 каналов проникновения плохих парней в вашу организацию?

1. E-mail
2. Web
3. Site-to-Site VPN
4. Remote Access VPN
5. Sharing resources
6. USB
7. Wi-Fi
8. Warez
9. BYOD
10. Embedded
11. Клиент-сервер с шифрованием
12. DevOps
13. Подрядчики
14. Уязвимость на портале
15. «Водопой» (Waterhole)
16. DNS
17. Облако

Что объединяет эти варианты?



- Кто/что, куда, когда и как
- География
- Web-логи
- Active Directory
- Приложения на узле

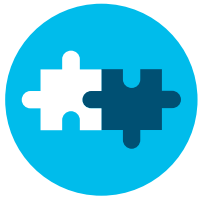
Cisco Stealthwatch

Осведомленность в реальном времени на ПК, филиалах, ЦОДах и облаках

Расширенная защита

Ускоренное реагирование

Простая сегментация



Stealthwatch Enterprise

Корпоративная сеть

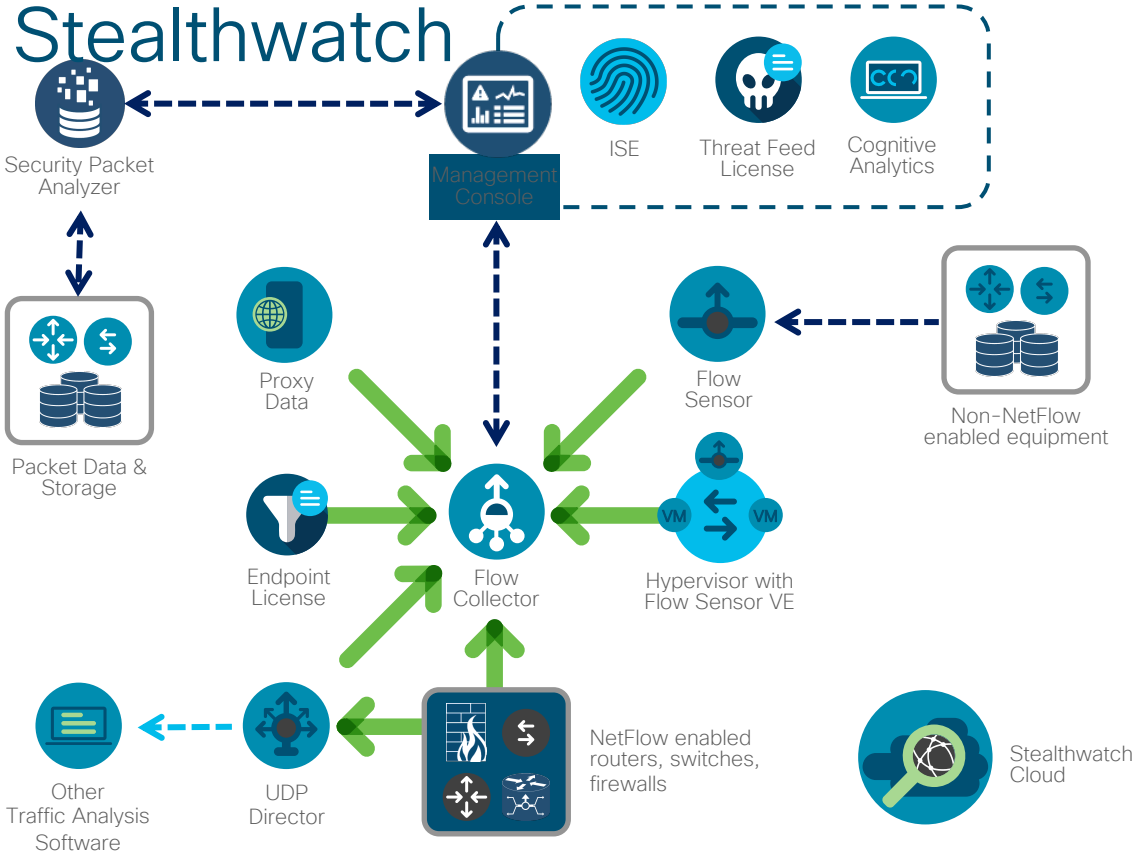
Частное облако

Stealthwatch Cloud

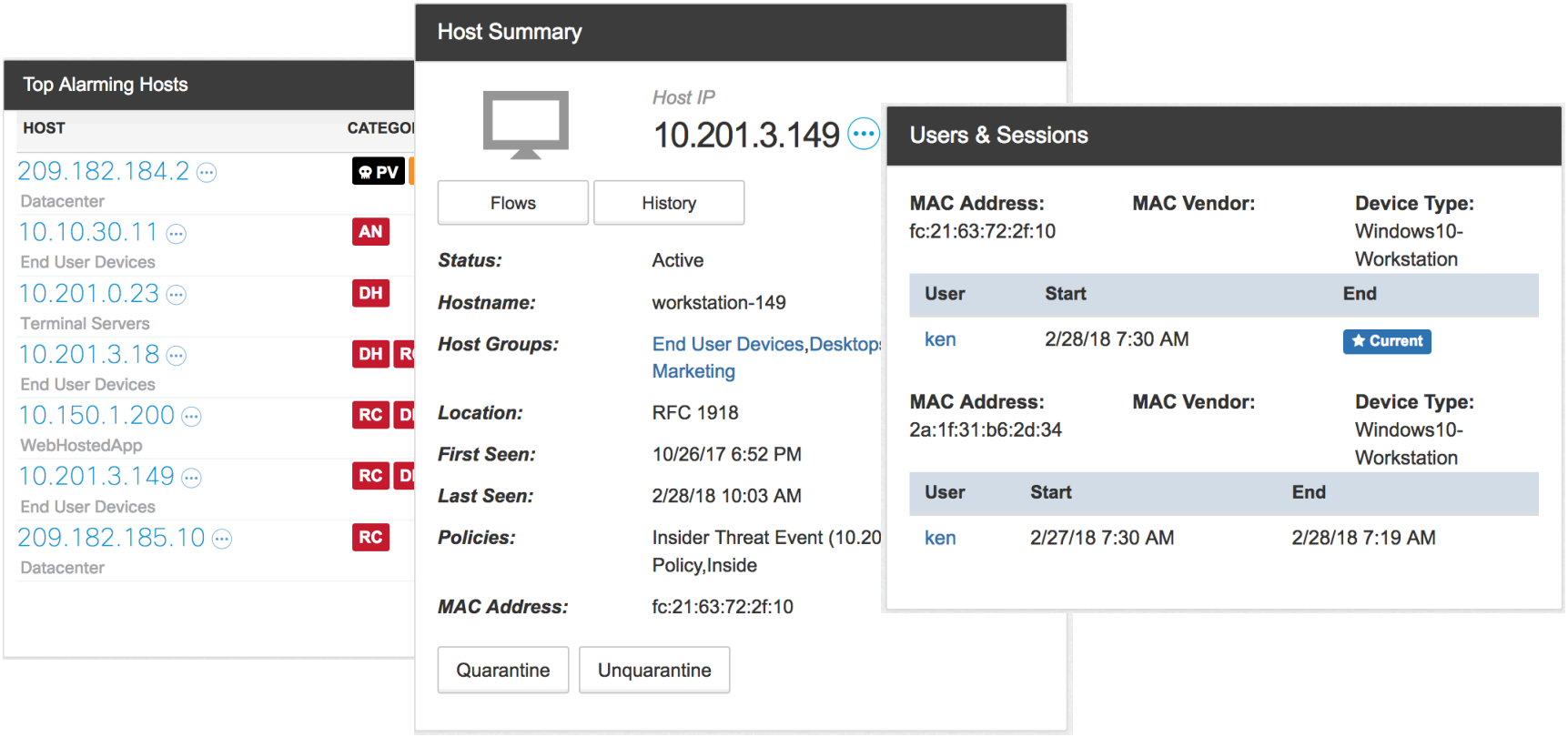
Публичное облако

Система Cisco Stealthwatch

Комплексная **безопасность** и сетевой **мониторинг**

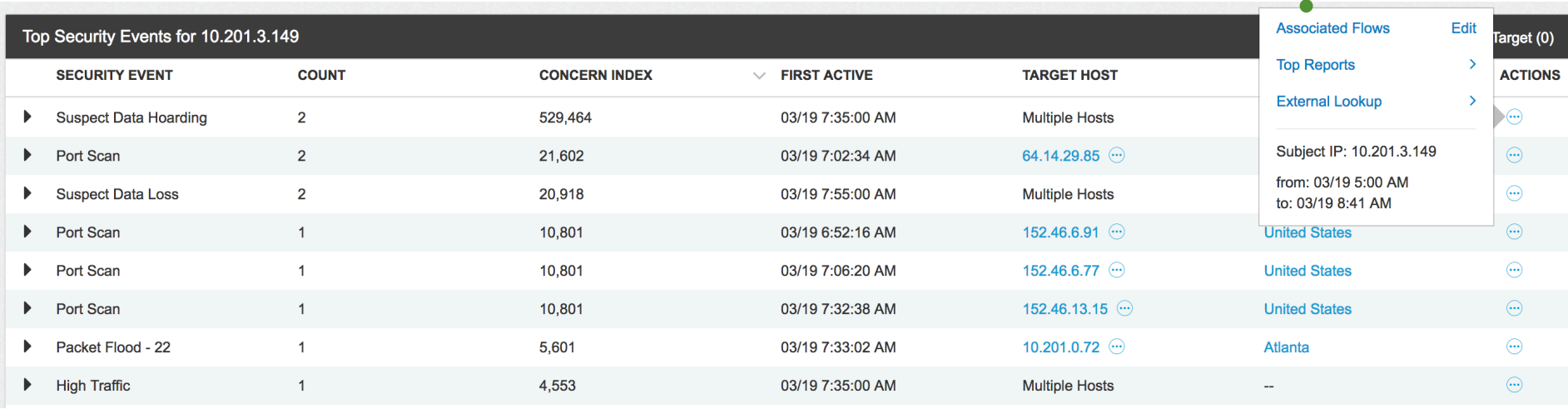


Внутренний нарушитель



Внутренний нарушитель крадет данные из ЦОДа

Дай мне все ассоциированные соединения?



Top Security Events for 10.201.3.149

	SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	TARGET HOST		ACTIONS
▶	Suspect Data Hoarding	2	529,464	03/19 7:35:00 AM	Multiple Hosts		
▶	Port Scan	2	21,602	03/19 7:02:34 AM	64.14.29.85		
▶	Suspect Data Loss	2	20,918	03/19 7:55:00 AM	Multiple Hosts		
▶	Port Scan	1	10,801	03/19 6:52:16 AM	152.46.6.91	United States	
▶	Port Scan	1	10,801	03/19 7:06:20 AM	152.46.6.77	United States	
▶	Port Scan	1	10,801	03/19 7:32:38 AM	152.46.13.15	United States	
▶	Packet Flood - 22	1	5,601	03/19 7:33:02 AM	10.201.0.72	Atlanta	
▶	High Traffic	1	4,553	03/19 7:35:00 AM	Multiple Hosts	--	

Внутренний нарушитель использует SSH

Manage Columns | Summary | Export

START	DURATION	SUBJECT IP A...	SUBJECT POR...	SUBJECT HOS...	SUBJECT BYTES	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/P...	PEER HOST G...
Ex. 06/0	Ex. <=50min	Ex. 10.10.10	Ex. 57100/U	Ex. "catch A	Ex. <=50M	Ex. "Corpora	Ex. <=50M	Ex. 10.255.2	Ex. 2055/UD	Ex. "Catch A
Mar 19, 2018 7:2... *(1hr 14min 7s ago)*	7min 13s	10.201.3.149	49780/TCP	End User Device...	12.69 M	SSH/SCP (uncla...	2.12 G	10.201.0.72	22/TCP	Atlanta
Mar 19, 2018 7:0... *(1hr 38min 40s a...*	4min 37s	10.201.3.149	49162/TCP	End User Device...	26.25 K	SSH/SCP (uncla...	66.31 K	10.201.0.72	22/TCP	Atlanta
Mar 19, 2018 6:3... *(2hr 4min 9s ago)*	31s	10.201.3.149	49162/TCP	End User Device...	8.18 K	SSH/SCP (uncla...	15.65 K	10.201.0.72	22/TCP	Atlanta
Mar 19, 2018 7:2... *(1hr 20min 27s a...*	2s	10.201.3.149	49162/TCP	End User Device...	364	SSH/SCP (uncla...	1012	10.201.0.72	22/TCP	Atlanta

Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend
SSH/SCP...	163.54 GB	76.00	1.15 GB		162.39 GB		
SSH	51.89 GB	24.00	504.62 MB		51.4 GB		

... а потом сливает все через HTTPS

Manage Columns | Export

% OF BYTES	HOST IP ADDR...	HOST NAME	HOST ROLE	PEER IP ADDR...	PEER NAME	PORT	BYTES	PACKETS	FLOWS	HOST BYTES ...	95T
10.4%	10.150.1.200	--	Client	173.199.5.25	--	443 / TCP (https)	3.48 G	4.57 M	1	85.22%	--
9.01%	10.150.1.200	--	Client	10.150.1.201	--	3306 / TCP (mysql)	3.02 G	3.33 M	1	1.7%	--
0.03%	10.150.1.200	--	Client	50.56.4.7	--	16384 / UDP (rtp)	11.72 M	64 K	1	0%	--
0.03%	10.150.1.200	--	Client	50.55.0.2	--	16384 / UDP (rtp)	11.68 M	63.8 K	1	0%	--

Анализ соединений – пример размножения сетевого червя...

Top Security Events for 10.110.10.254 — Source (10) | Target (1)

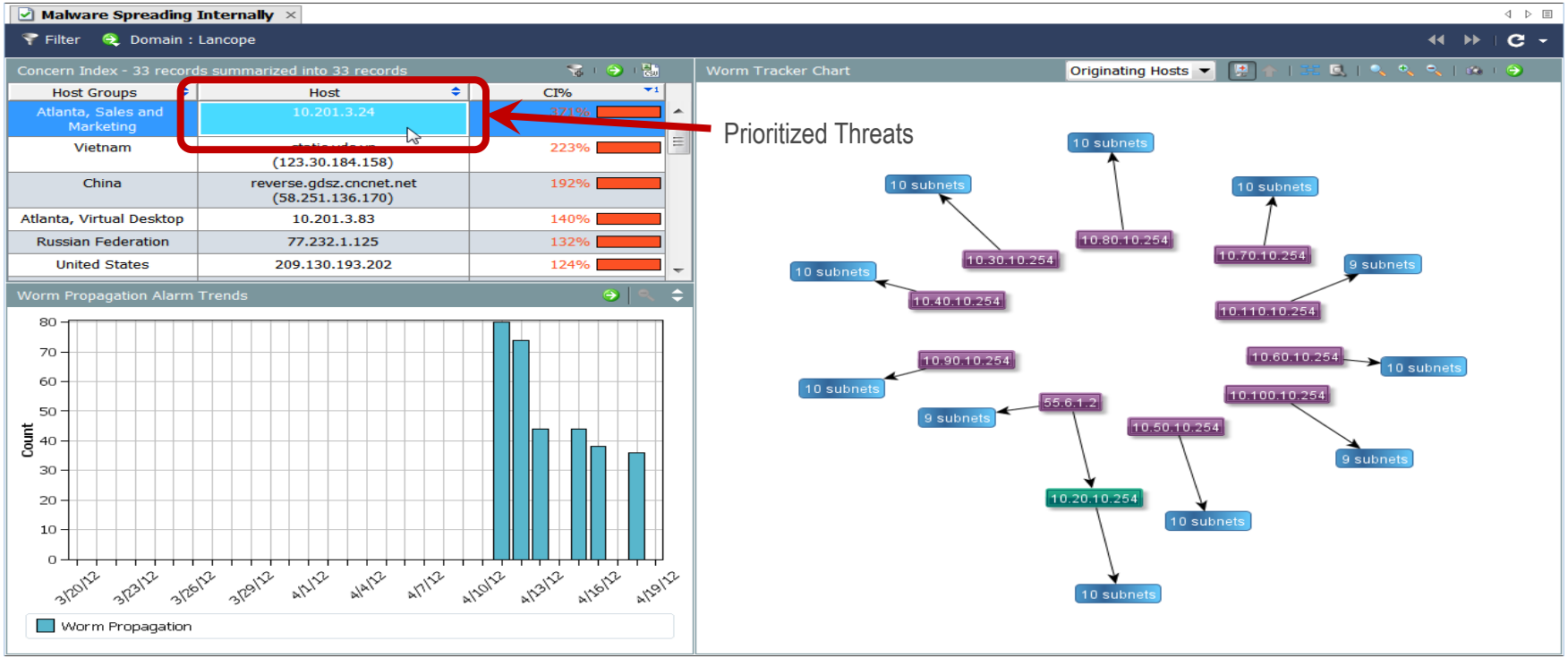
SECURITY EVENT	COUNT	CONCERN INDEX	FIRST ACTIVE	TARGET HOST	TARGET HOST GROUP	ACTIONS
Addr_Scan/tcp - 5900	5,154	3,441,154	03/06 8:29:16 AM	10.120.30.0/24	End User Devices , Desktops , ...	
Addr_Scan/tcp - 5900	4,950	3,304,950	03/06 8:29:16 AM	10.120.40.0/24	End User Devices , Desktops , ...	
Addr_Scan/tcp - 5900	4,890	3,264,890	03/06 8:29:15 AM	10.120.20.0/24	End User Devices , Desktops , ...	
Addr_Scan/tcp - 5900	4,332	2,892,332	03/06 8:29:14 AM	10.120.10.0/24	End User Devices , Desktops , ...	
Addr_Scan/tcp - 5900	4,266	2,848,266	03/06 8:29:19 AM	10.120.60.0/24	End User Devices , Desktops , ...	
Addr_Scan/tcp - 5900	4,158	2,776,158	03/06 8:29:18 AM	10.120.50.0/24	End User Devices , Desktops , ...	
Addr_Scan/tcp - 5900	4,068	2,716,068	03/06 8:29:20 AM	10.120.70.0/24	End User Devices , Desktops , ...	
Addr_Scan/tcp - 5900	3,630	2,423,630	03/06 8:29:22 AM	10.120.80.0/24	End User Devices , Desktops , ...	
Addr_Scan/tcp - 5900	3,486	2,327,486	03/06 8:29:24 AM	10.120.100.0/24	End User Devices , Desktops , ...	
Worm Propagation - 5900	9	172,809	03/06 8:34:31 AM	10.120.20.254	End User Devices , Desktops , ...	

DETAILS
--

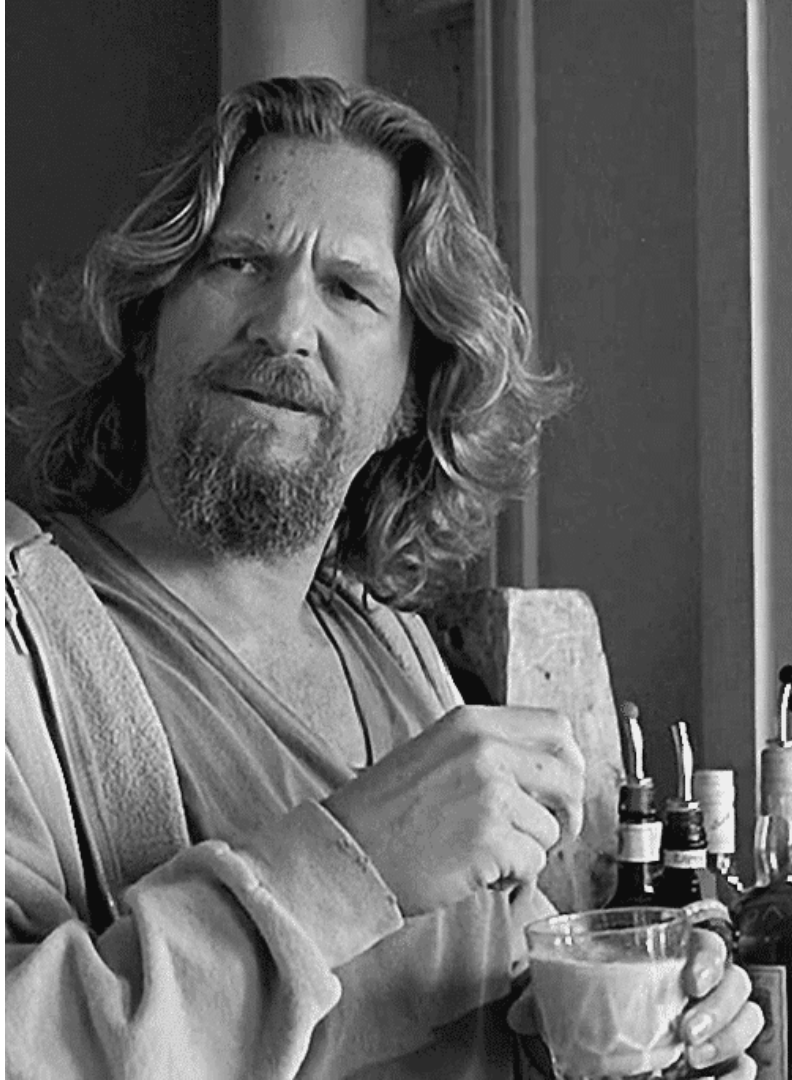
DESCRIPTION
Addr_Scan/tcp - 5900: The source host is attempting to contact multiple hosts (using TCP) within a natural class C network (/24) on the same port and most connection attempts are either being rejected (TCP Reset) or the target hosts are not responding at all. This is used to trigger the Worm Activity and Worm Propagation alarms. These are commonly seen during network scanning or enumeration.

View More Security Events >

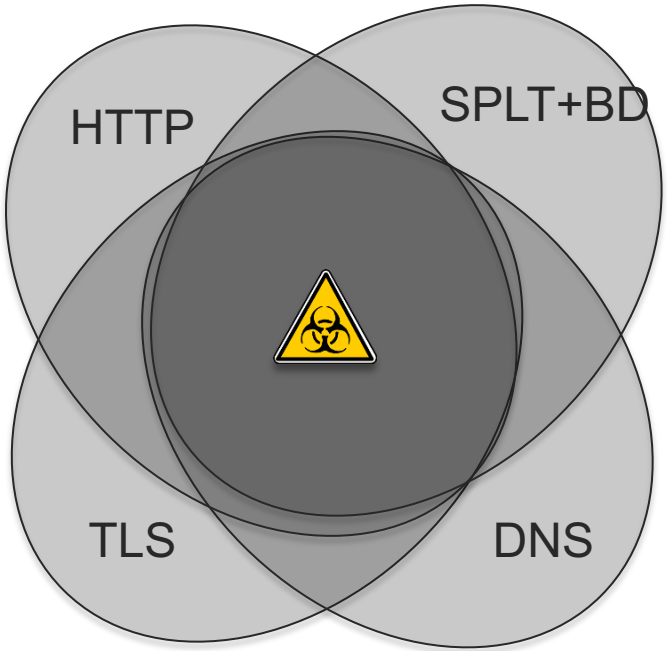
...или визуально



Обнаружение вредоносного кода, использующего шифрование, с помощью сетевой телеметрии – без расшифровки трафика

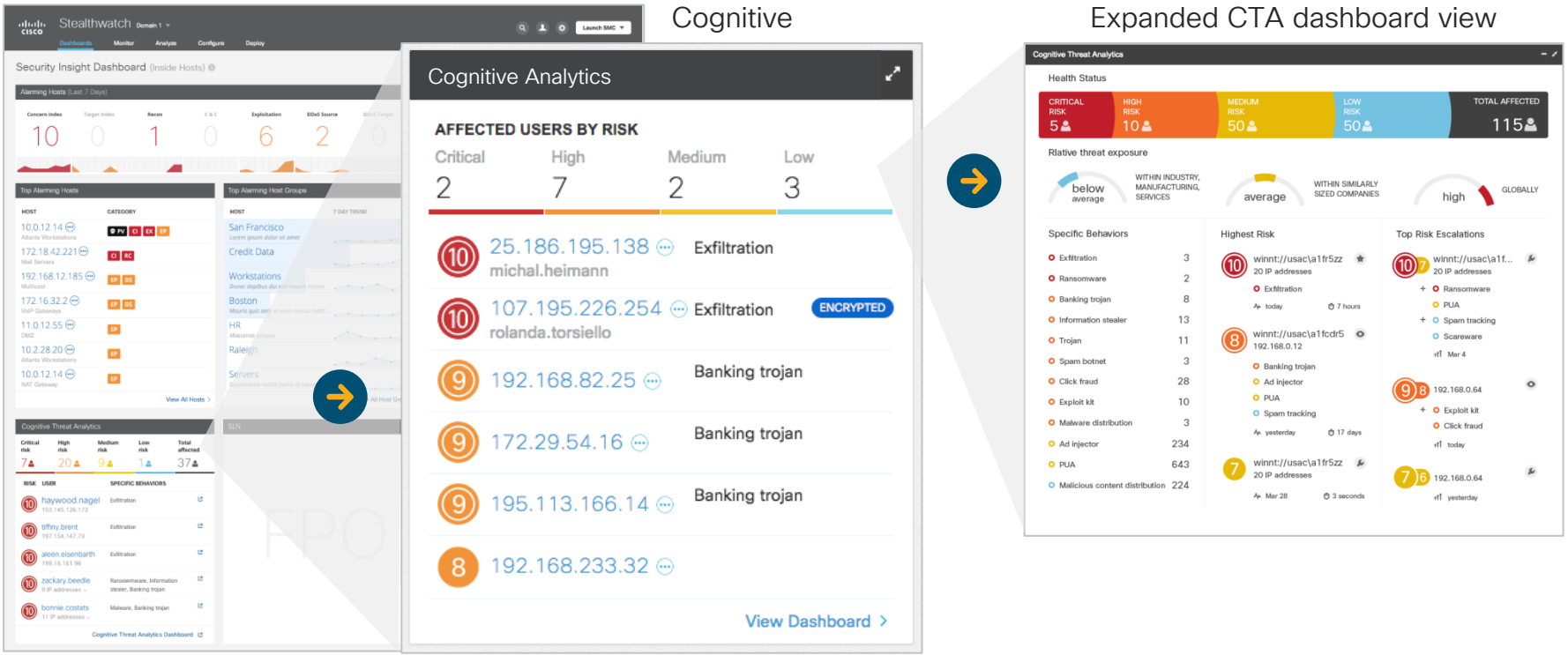


Эффективность обнаружения ВПО в шифрованном трафике



	Acc.	FDR
SPLT+BD+TLS+HTTP+DNS	99.993%	99.978%
SPLT+BD+TLS+HTTP	99.983%	99.956%
SPLT+BD+TLS+DNS	99.968%	98.043%
SPLT+BD+TLS	99.933%	70.351%
HTTP+DNS	99.985%	99.956%
TLS+HTTP	99.955%	99.660%
TLS+DNS	99.883%	96.551%
HTTP	99.945%	98.996%
DNS	99.496%	94.654%
TLS	94.836%	50.406%

Обнаружение зашифрованного вредоноса



Cognitive

Expanded CTA dashboard view

Cisco Stealthwatch

ETA Анализ зашифрованного трафика во внутренней корпоративной сети

ROI Защита сделанных инвестиций в сетевую инфраструктуру и возможность использования решения для ИТ и ИБ

Не требует перестройки сети для мониторинга внутренних угроз

Мониторинг инфраструктуры Cisco и не только (IPFIX, cFlow, jFlow, sFlow)

От мониторинга к предотвращению

НЕИЗВЕСТНО

Отсутствие контекста		Богатый контекст
IP ADDRESS: 192.168.2.101		Дмитрий Казаков (СОТРУДНИК)
НЕИЗВЕСТНО		WINDOWS WORKSTATION
НЕИЗВЕСТНО		ЗДАНИЕ-А-ЭТАЖ-13
НЕИЗВЕСТНО		10:30 AM MSK APR 27
НЕИЗВЕСТНО		БЕСПРОВОДНАЯ СЕТЬ
НЕИЗВЕСТНО		НЕТ УГРОЗ / УЯЗВИМОСТЕЙ

ИЗВЕСТНО

РЕЗУЛЬТАТ	РЕЗУЛЬТАТ
ДОСТУП К IP (ЛЮБОЕ УСТРОЙСТВО / ПОЛЬЗОВАТЕЛЬ)	РОЛЕВОЙ ДОСТУП

На периметре вы обычно ставите МСЭ (FW) и СОВ (IDS)!

- Если Cisco Stealthwatch – это система обнаружения атак во внутренней инфраструктуре, то есть ли у Cisco внутренний межсетевой экран?
- И чтобы он задействовал внутреннюю инфраструктуру!
- И чтобы он был прост в управлении!
- И чтобы он интегрировался с периметром!

Да! Это – Cisco Identity Services Engine!

Централизованное решение для автоматизации контекстно-задаваемых политик доступа к сетевым ресурсам и обмена контекстом

Спасибо за внимание!

security-request@cisco.com