ИНФОСИСТЕМЫ ДЖЕТ

ЛЕТ
ФОРМИРУЕМ ТРЕНДЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

«Джет» – навигатор по рынку анти-APT

Юрий Черкас,
менеджер по развитию бизнеса
Центра информационной безопасности

Как это было 1 апреля

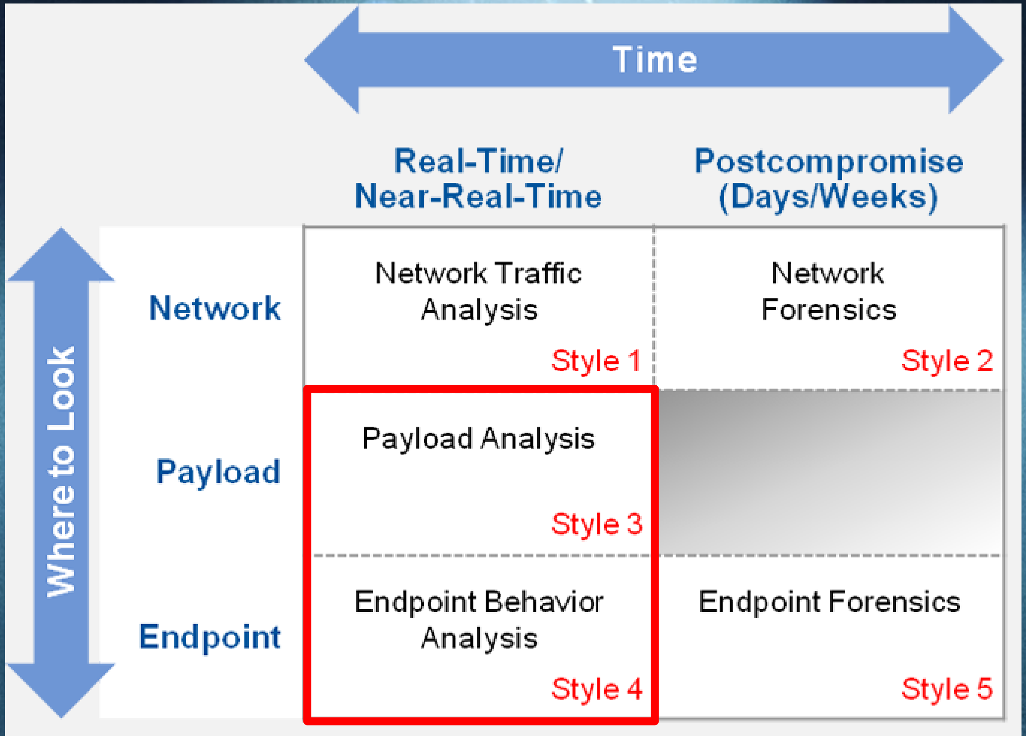
Защита от APT по Gartner

Time

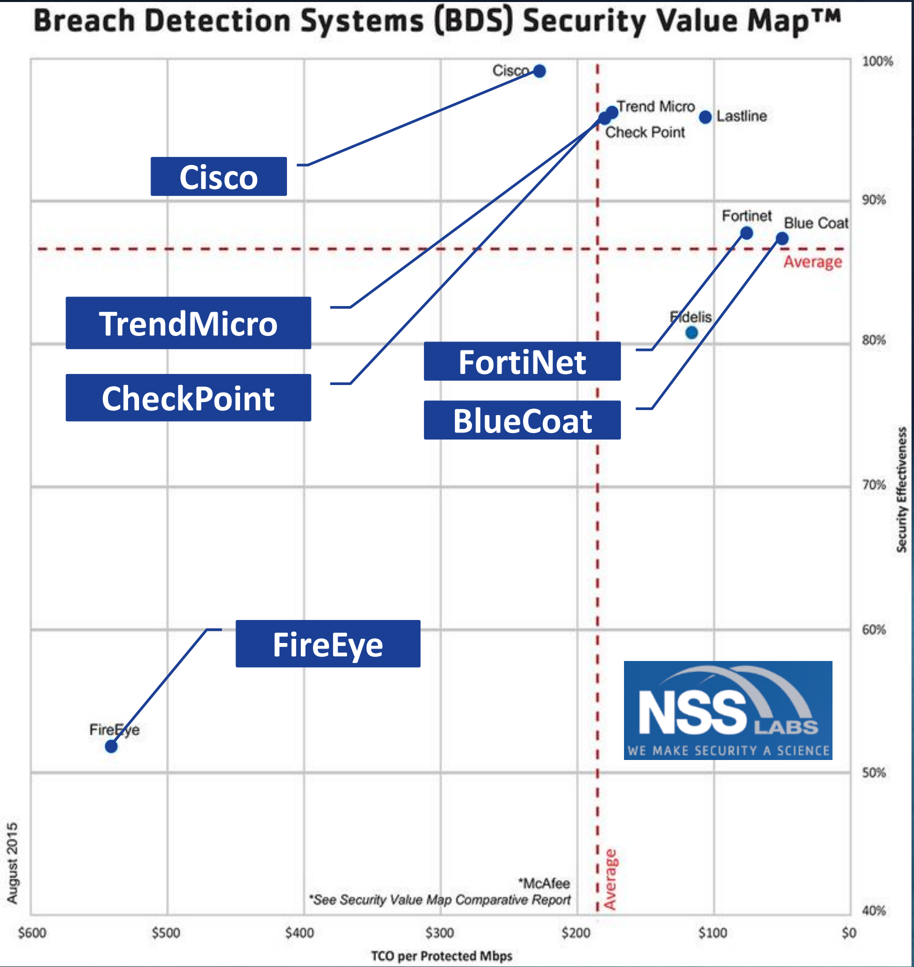
Where to Look	Real-Time/ Near-Real-Time	Postcompromise (Days/Weeks)
Network	Network Traffic Analysis Style 1	Network Forensics Style 2
Payload	Payload Analysis Style 3	
Endpoint	Endpoint Behavior Analysis Style 4	Endpoint Forensics Style 5

Gartner выделяет 5 стилей защиты

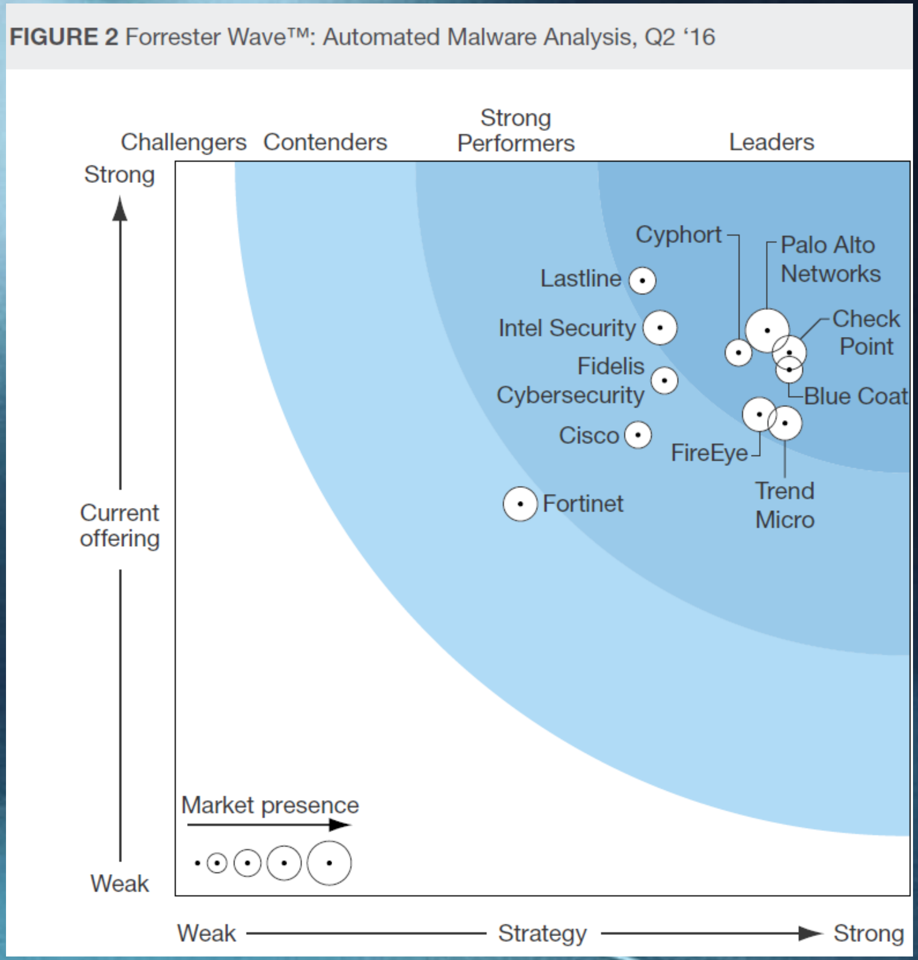
Style 3-4


Time
Real-Time/
Near-Real-Time
Postcompromise
(Days/Weeks)
Where to Look
Network
Payload
Endpoint
Network Traffic
Analysis
Style 1
Network
Forensics
Style 2
Payload Analysis
Style 3
Endpoint Behavior
Analysis
Style 4
Endpoint Forensics
Style 5

NSS Labs & Forrester Wave



- CheckPoint
- TrendMicro
- PaloAlto
- FortiNet
- BlueCoat
- Cisco
- FireEye



Навигация по песочницам

О своем подходе расскажут:

FireEye

Check Point
SOFTWARE TECHNOLOGIES LTD.

Jet infosystems

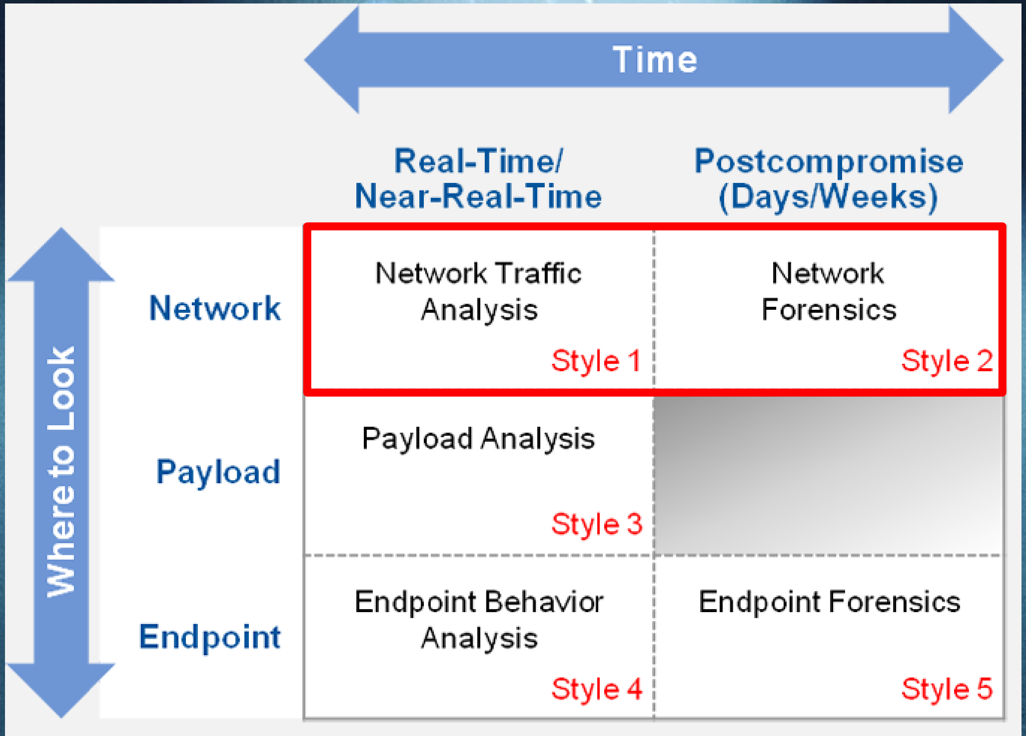
Расскажет:

Про критерии сравнения на примере:

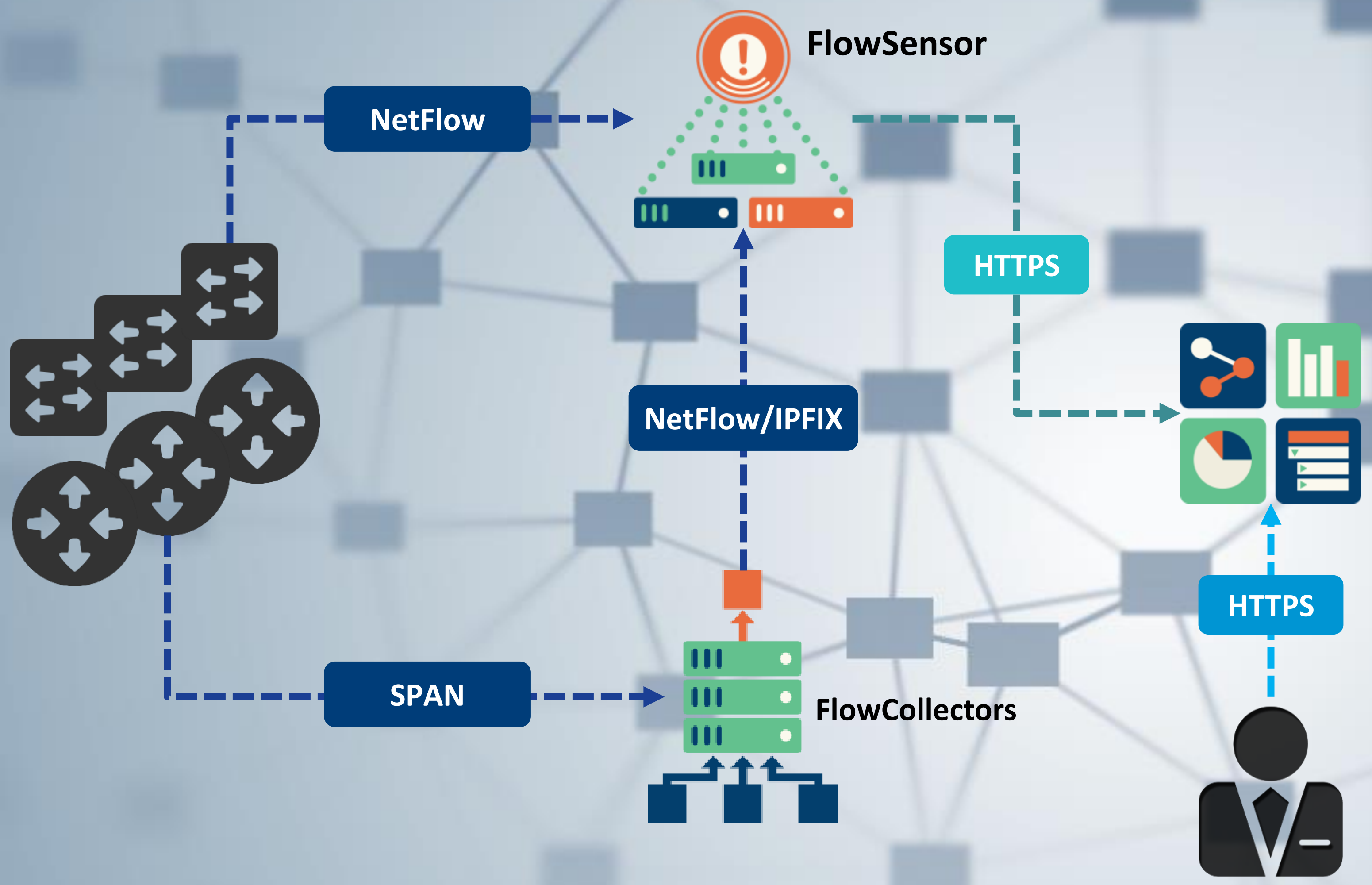
- FireEye
- CheckPoint
- TrendMicro
- Kaspersky ATA

TOP SECRET

Style 1-2

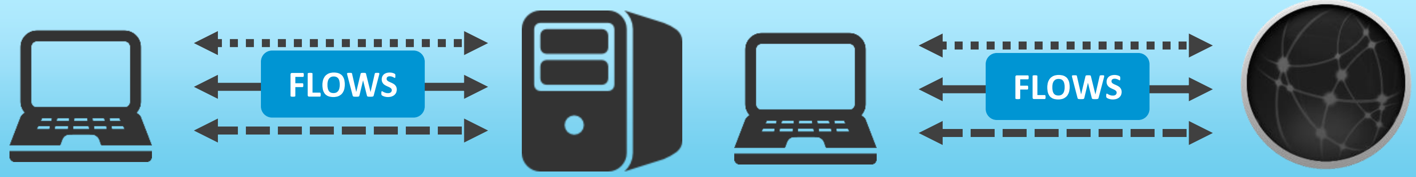

Time
Real-Time/
Near-Real-Time
Postcompromise
(Days/Weeks)
Where to Look
Network
Payload
Endpoint
Network Traffic
Analysis
Style 1
Network
Forensics
Style 2
Payload Analysis
Style 3
Endpoint Behavior
Analysis
Style 4
Endpoint Forensics
Style 5

Network Behavior Analyses или Style 1



Принцип работы NBA

Сбор и анализ потоков



Построение шаблонов поведения

Более 80 параметров

Сигнатуры приложений

Мониторинг поведения и выявление аномалий

Основные игроки

Network Behavior Analyses

Vol XCIII, No. 311 Thursday, June 02, 2016 $1.25

Arbor Networks Spectrum

ARBOR NETWORKS

Introducing Arbor Networks Spectrum: The Advanced Threat Platform that Connects Attacks Across the Internet with Internal Enterprise Networks

Empowering security teams to find and prove active attack campaigns 10x more effectively than SIEM and Security Forensics

Flowmon Networks

Flowmon Networks

inveaTECH

MANAGE AND SECURE YOUR IT ENVIRONMENT WITH CONFIDENCE

Performance issues, unavailability of critical application, security breaches. All of that can cause financial loss, reputation damage, employee dissatisfaction and churn of customers.

Cisco Cyber Threat Defense

CISCO

Lancope.

Stronger Protection Against Advanced Threats

Advanced threats can breach even the best security perimeter and penetrate your network undetected. And they even may hide for a while until they begin to do damage. Over time, they conduct a sophisticated strategic campaign that may use multiple methods.

Defense against this type of attack requires a new approach. You need network visibility, control, context, and intelligence. You need to understand a threat that has gained an operational footprint on the network interior and learn how it is operating.

Cisco Cyber Threat Defense is an advanced threat detection and response system. With it, you can reduce both the probability of an attack and the time to discovery and remediation of the threat. It is a Cisco Validated Design that encompasses the entire Cisco security portfolio and integrates into the fabric of the Cisco network.

Cyber Threat Defense detects, tracks, exposes, and quarantines advanced threats using the following automated capabilities

Time

Where to Look

	Real-Time/ Near-Real-Time	Postcompromise (Days/Weeks)
Network	Network Traffic Analysis Style 1	Network Forensics Style 2
Payload	Payload Analysis Style 3	
Endpoint	Endpoint Behavior Analysis Style 4	Endpoint Forensics Style 5

Style 1’

Anti-Bot = Anti-APT ?

1. **События передаются в центр анализа**
2. **Специалисты вручную анализируют, классифицируют и выделяют важное**

ИНФОСИСТЕМЫ ДЖЕТ

ЛЕТ

ФОРМИРУЕМ ТРЕНДЫ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Начнем навигацию!