The Critical Role of Netflow/IPFIX Telemetry in the Next-Generation Network Security Infrastructure

Ken Kaminski, Technical Solutions Architect – Northeast

Cisco Systems

CISSP, GAWN, GPEN, GCIA, GCFA, GMOB

June 2015

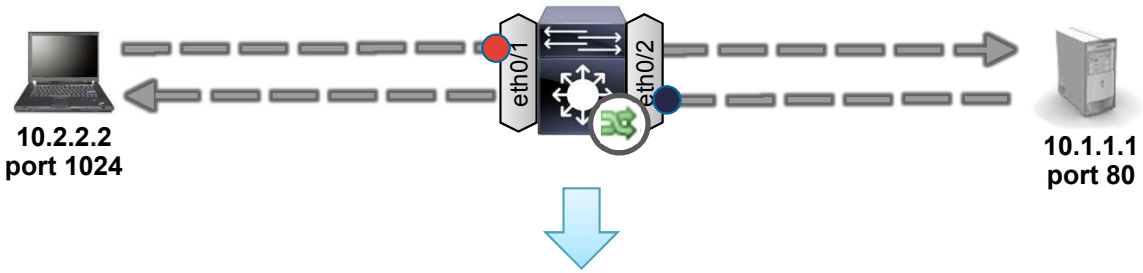
Agenda

Introduction – Big Picture
Netflow Fundamentals
Design
Adding Context

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

Introduction – Big Picture

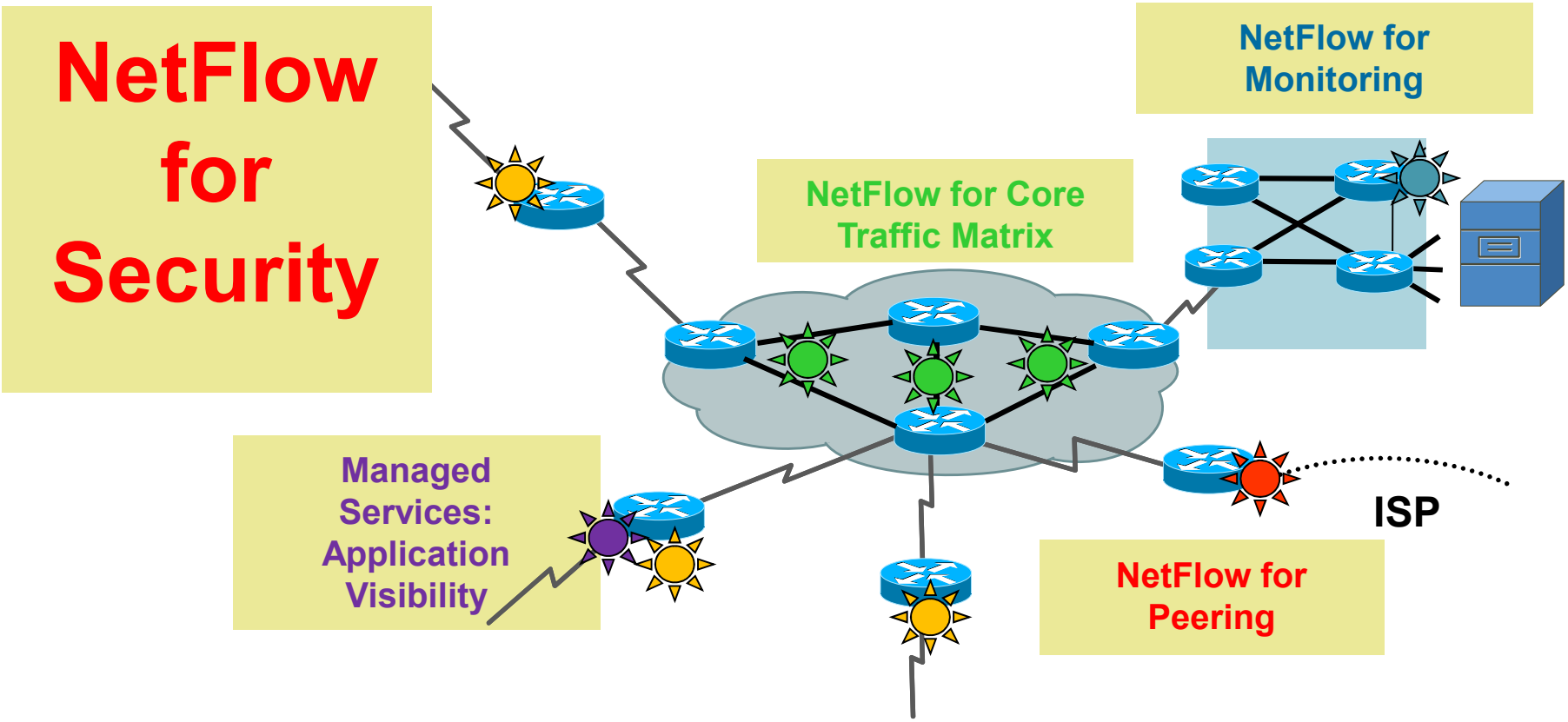
NetFlow



Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent	TCP Flags
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025	SYN,ACK,PSH
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712	SYN,ACK,FIN

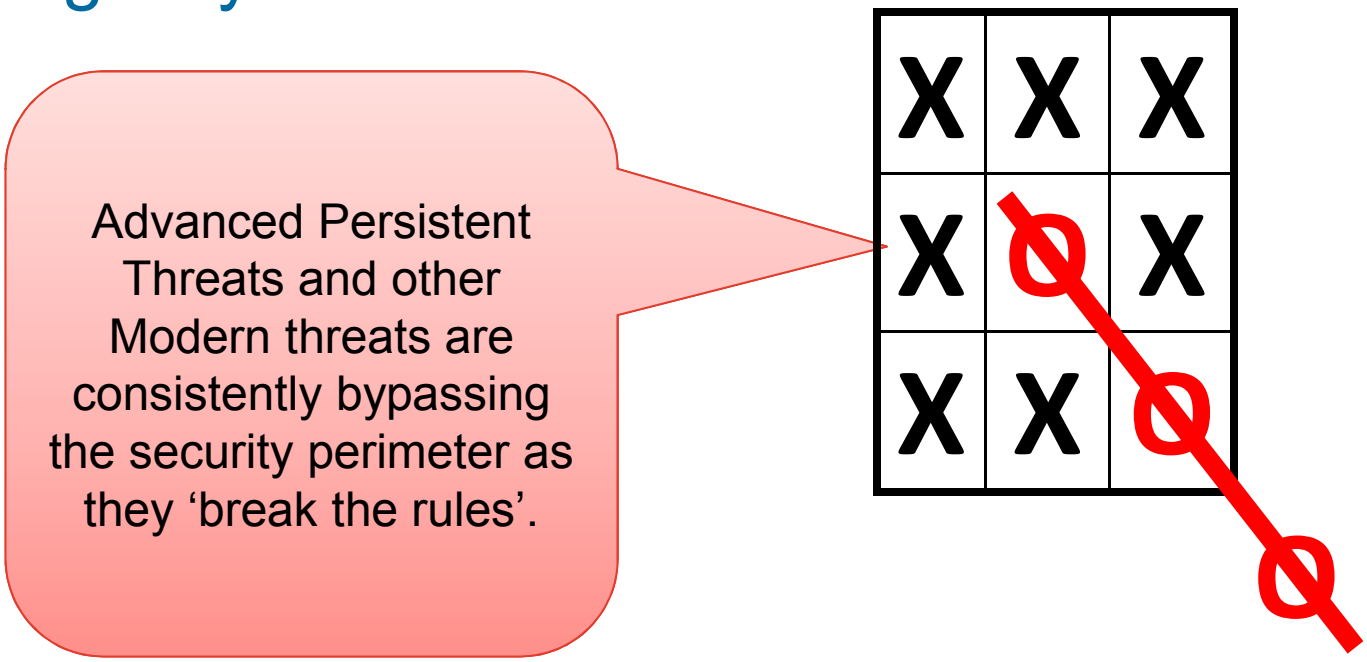
© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

Typical NetFlow Deployment



© 2014 Cisco and/or its affiliates. All rights reserved.

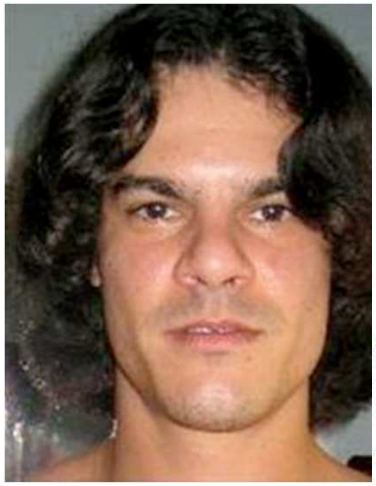
Thinking Beyond the Perimeter



An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing and the financial industry.

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

Defending against Humans



http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

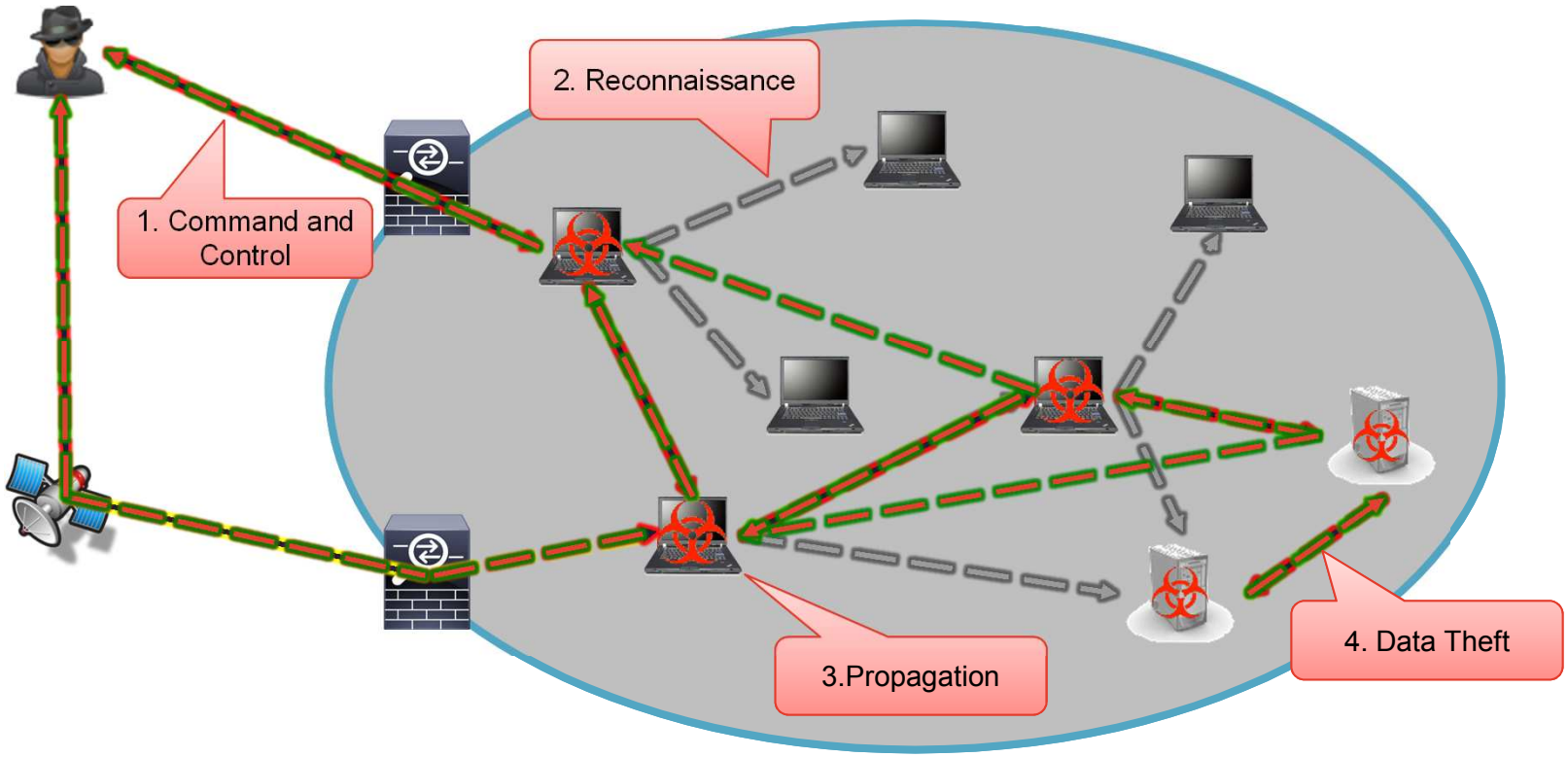
Concept: Kill Chain

Reconnaissance	•Harvesting email addresses, identifying information, etc.
Weaponization	•Coupling exploit with backdoor into deliverable payload
Delivery	•Delivering weaponized bundle to the victim via email, web, USB, etc.
Exploitation	•Exploiting a vulnerability to execute code in victim system
Command and Control	•Command channel for remote manipulation of victim
Actions on Objectives	•Intruders accomplish their original goal: Lateral movement, data exfiltration (collect, encrypt, and extract)

- http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/
- http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

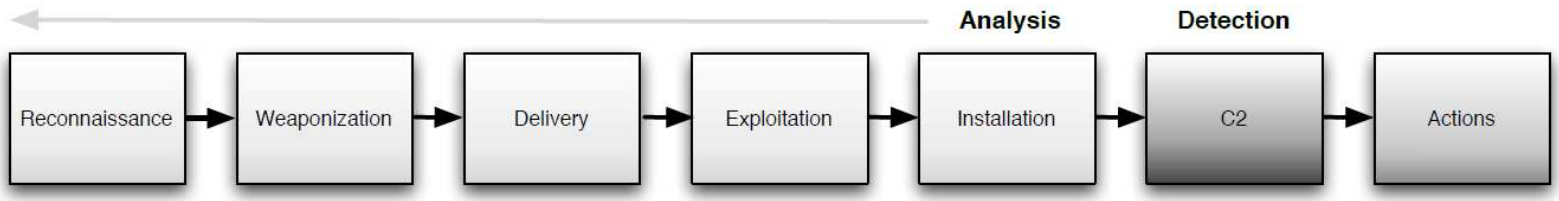
Kill Chain: Post Breach



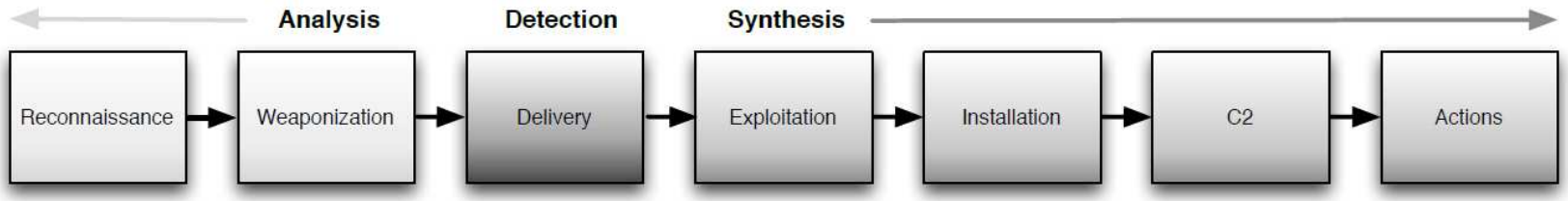
© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

Goal: Early Phase Detection

Late Phase Detection



Earlier Phase Detection



http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

© 2014 Cisco and/or its affiliates. All rights reserved.

Signals Intelligence

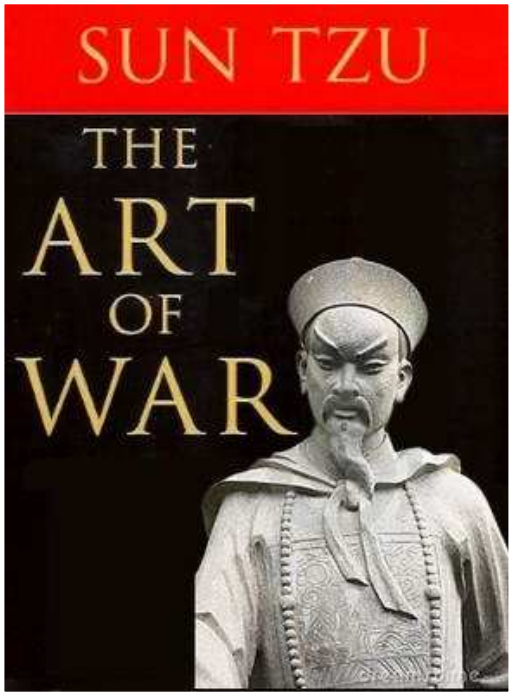
Traffic Analysis:

- Deduce information from communication patterns

© 2014 Cisco and/or its affiliates. All rights reserved.

"If ignorant of both of your enemy and yourself, you are certain to be in peril."

Sun Tzu



Visibility of all host-to-host communication, inside and out, is essential to the maintenance of a strong security posture.

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

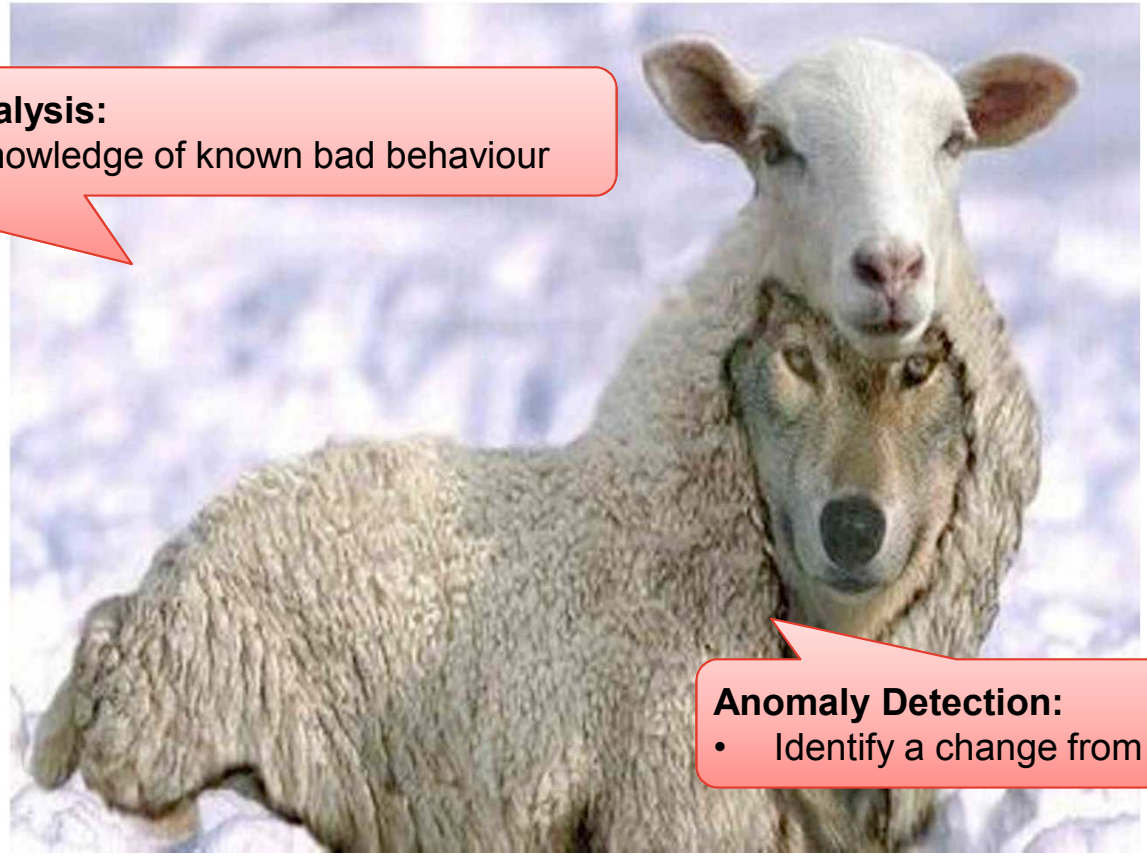
NetFlow = Visibility

A single NetFlow Record provides a wealth of information

```
Router# show flow monitor CYBER-MONITOR cache
...
IPV4 SOURCE ADDRESS:        192.168.100.100
IPV4 DESTINATION ADDRESS:   192.168.20.6
TRNS SOURCE PORT:           47321
TRNS DESTINATION PORT:      443
INTERFACE INPUT:            Gi0/0/0
IP TOS:                     0x00
IP PROTOCOL:                6
ipv4 next hop address:      192.168.20.6
tcp flags:                  0x1A
interface output:           Gi0/1.20
counter bytes:              1482
counter packets:            23
timestamp first:            12:33:53.358
timestamp last:             12:33:53.370
ip dscp:                    0x00
ip ttl min:                 127
ip ttl max:                 127
application name:           nbar secure-http
...
```

© 2014 Cisco and/or its affiliates. All rights reserved.

Behavioural Analysis & Anomaly Detection



Behavioural Analysis:
- Leverages knowledge of known bad behaviour

Anomaly Detection:
- Identify a change from “normal”

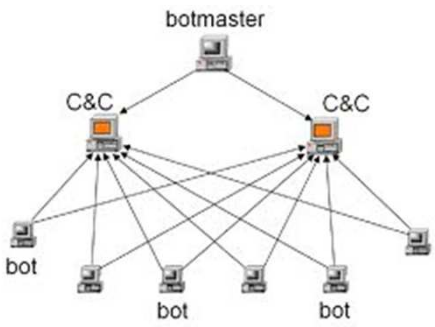
© 2014 Cisco and/or its affiliates. All rights reserved.

Network Behaviour Anomaly Detection (NBAD)

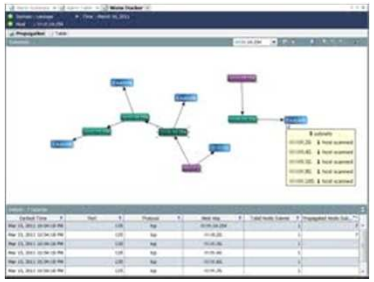
	Signature	Behaviour	Anomaly
Known Exploits	**Best**	Good	Limited
0-Day Exploits	Limited	**Best**	Good
Credential Abuse (Insider Threat)	Limited	Limited	**Best**

© 2014 Cisco and/or its affiliates. All rights reserved.

Attack Penetration, Propagation, and Exfiltration



Botnet Command And Control



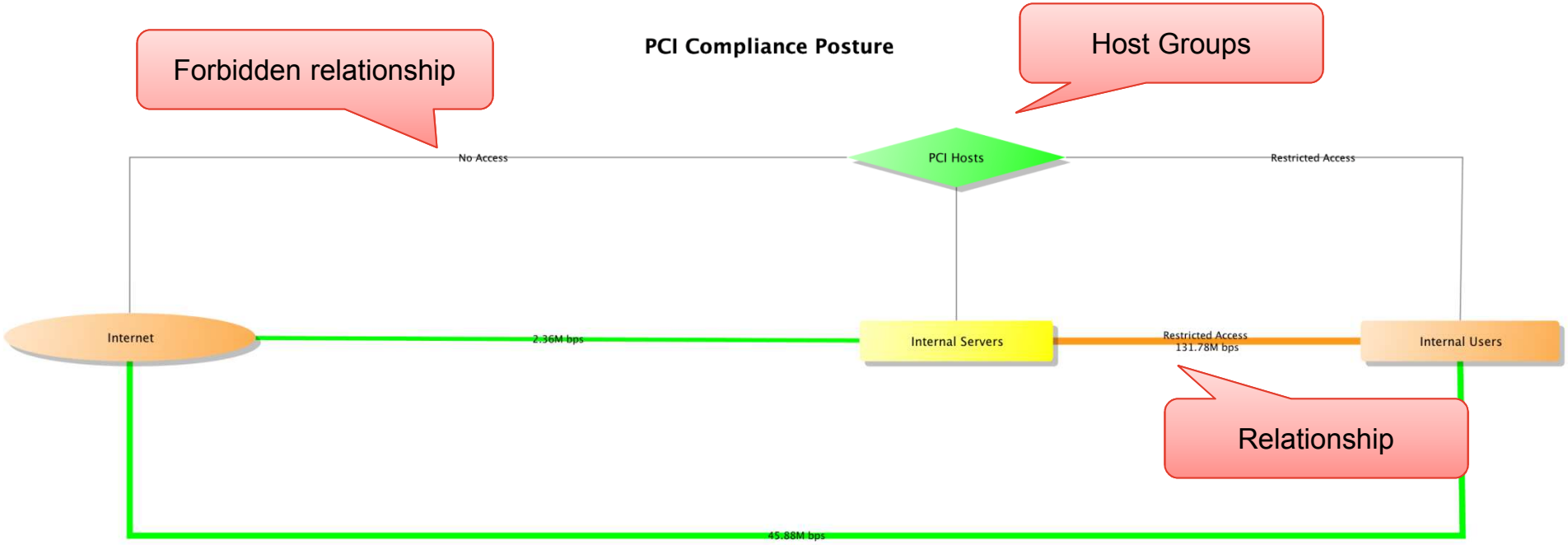
Internally Propagating Malware

Network Reconnaissance

Data Leakage – Data Hoarding and Data Exfiltration

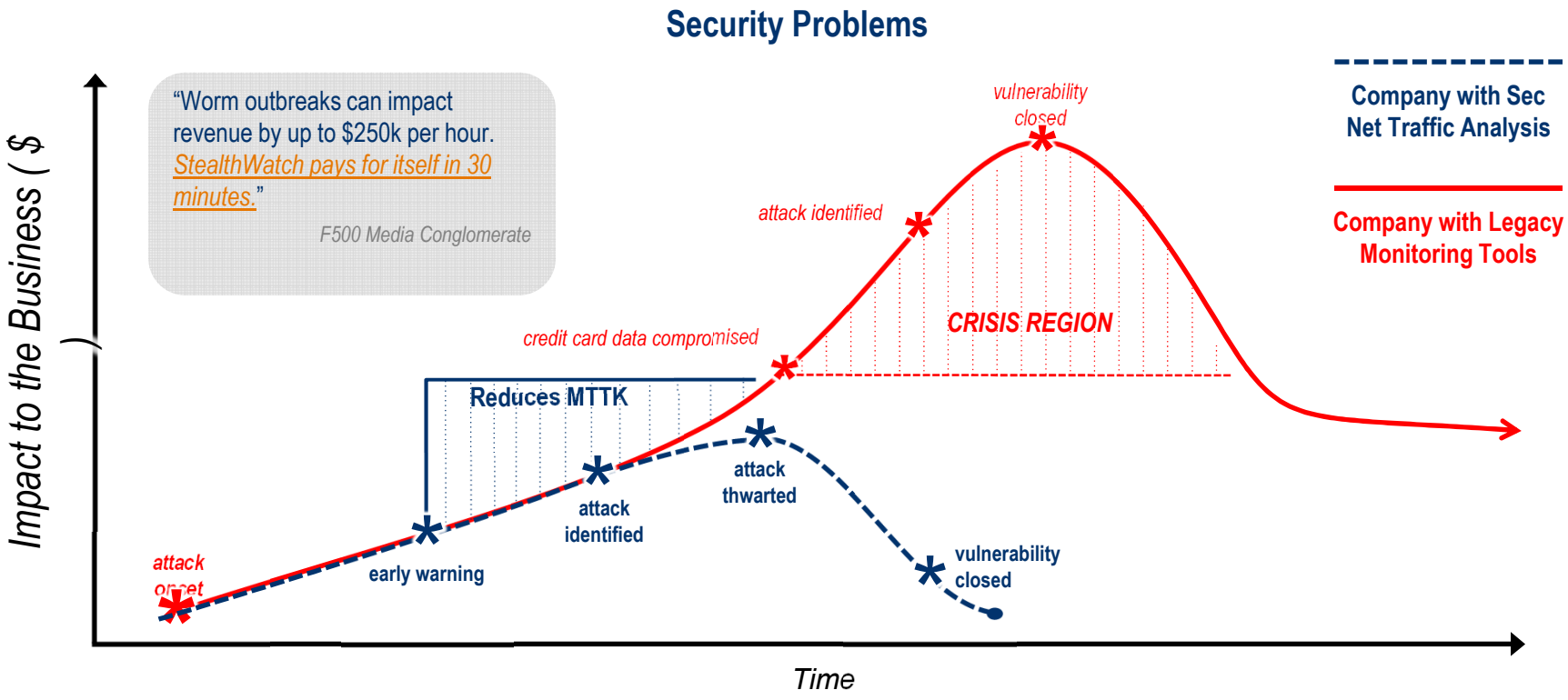
© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

Relational Flow Maps



© 2014 Cisco and/or its affiliates. All rights reserved.

Stop Security Problems *BEFORE* They Become Crises



© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

Gartner: 'Five Styles of Advanced Threat Defense' can protect enterprise from targeted attacks – Aug 2013

1. **Network Traffic Analysis techniques (Lancope, Arbor, Cisco AMP)**
2. Network Forensics - "full-packet capture and storage of network traffic" (RSA NetWitness)
3. Payload Analysis - sandbox techniques (FireEye)
4. Endpoint Behavior Analysis – agent on every endpoint: HIPS, memory monitoring
5. Endpoint Forensics - tools for incident response teams: Endpoint Detection & Response Tools (Bit9 Carbon Black, Cisco AMP, Guidance Encase)

- <u>Gartner recommends using two of the above five at least</u>
- General Requirement: analyze network traffic for compromised hosts

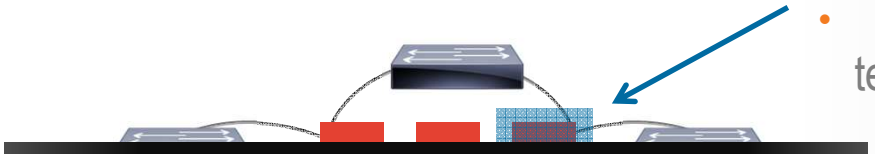
© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ponemon Report: Cyber Security Incident Response

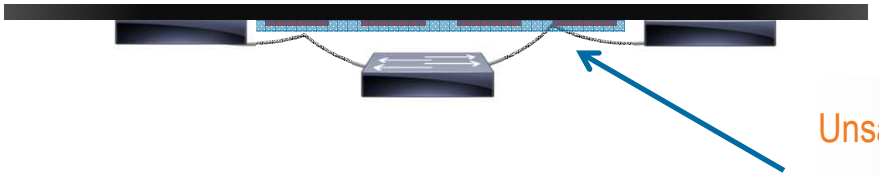
- Ponemon report highlighting the value of NBAD - http://www.lancope.com/resources/industry-report/ponemon-institute-report-cyber-security-incident-response-are-we-prepared
- Network audit trails are the most effective tool for incident response.
- 80% of respondents indicated that analysis of audit trails from sources like NetFlow and packet captures was the most effective approach for detecting security incidents and breaches.

© 2014 Cisco and/or its affiliates. All rights reserved.

Unsampled NetFlow: Key to the Solution



Want Switch to Deliver Unsampled NetFlow at Line-Rate Without Any Data Plane Performance Impact



Sampled NetFlow – Incomplete Visibility

- Less than 5% of traffic used to generate NetFlow telemetry
- Insufficient telemetry for threat detection

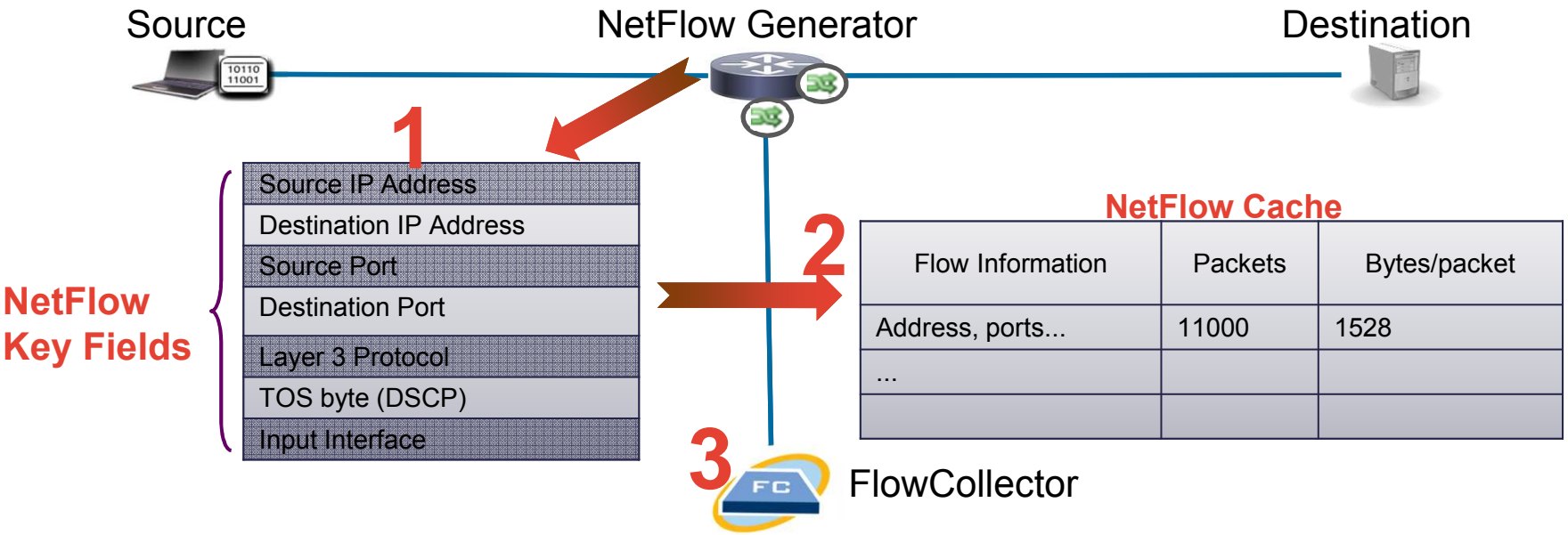
Unsampled NetFlow – **No Blind Spots**

- All traffic is used to generate NetFlow telemetry
- Pre-requisite for effective threat detection

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

Netflow Fundamentals

Introduction to NetFlow



1. Inspect a packets key fields and identify the values
2. If the set of key field values are unique create a cache entry
3. On termination or timeout export a flow record to the collector

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

NetFlow v5 and NetFlow v9

Which to Use for Threat Detection?

NetFlow v5

NetFlow v5 Captures Essential Information Regarding Traffic Patterns

- Source/dest IP and port
- Packet counts
- Byte counts
- Flow duration
- I/O interfaces

Useful for Layers 3 and 4 Traffic Pattern Analysis

NetFlow v9

NetFlow v9 Extends NetFlow v5 by Adding:

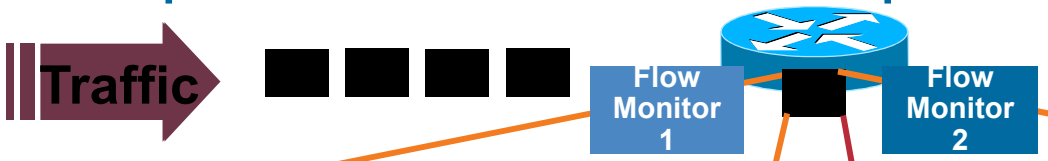
- Numerous TCP flags/counters
- Flow direction
- Fragmentation flags
- ICMP and IGMP info
- Header stats
- Time-to-live
- DSCP/TOS info
- Destination routing info

Provides Insight to Malformed Packets, Protocol Manipulation, and Direction of Traffic

NetFlow v5 Is Useful, However, NetFlow v9 Delivers Deeper Insight

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

Flexible NetFlow
Multiple Monitors with Unique Key Fields



Key Fields	Packet 1
Source IP	3.3.3.3
Destination IP	2.2.2.2
Source Port	23
Destination Oort	22078
Layer 3 Protocol	TCP - 6
TOS Byte	0
Input Interface	Ethernet 0

Non-Key Fields
Packets
Bytes
Timestamps
Next Hop Address

Key Fields	Packet 1
Source IP	3.3.3.3
Dest IP	2.2.2.2
Input Interface	Ethernet 0
SYN Flag	0

Non-Key Fields
Packets
Timestamps

Traffic Analysis Cache

Source IP	Dest. IP	Source Port	Dest. Port	Protocol	TOS	Input I/F	…	Pkts
3.3.3.3	2.2.2.2	23	22078	6	0	E0	…	1100

Security Analysis Cache

Source IP	Dest. IP	Input I/F	Flag	…	Pkts
3.3.3.3	2.2.2.2	E0	0	…	11000

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

NetFlow Terminology

- Flow Exporter
  - The process that will export NetFlow data to a collector
- Flow Record
  - Definition of the key and non-key fields that will be collected from a flow
  - Key fields: configured using the match option
  - Non-key fields: configured using the collect option
- Flow Monitor
  - This defines the process that manages the NetFlow cache on the device
  - Configuration links the Flow Exporter and the Flow record definition together
  - A flow monitor is applied to an interface to enable NetFlow on the interface

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

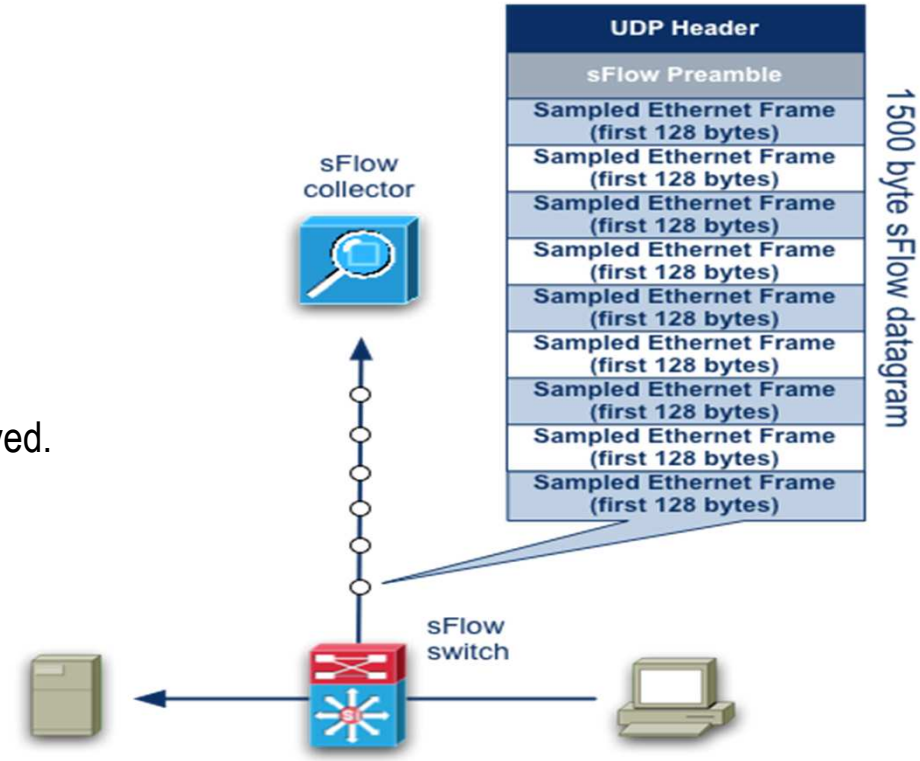
Versions of NetFlow

Version	Major Advantage	Limits/Weaknesses
V5	Defines 18 exported fields Simple and compact format Most commonly used format	IPv4 only Fixed fields, fixed length fields only Single flow cache
V9	Template-based IPv6 flows transported in IPv4 packets MPLS and BGP nexthop supported Defines 104 fields, including L2 fields Reports flow direction	IPv6 flows transported in IPv4 packets Fixed length fields only Uses more memory Slower performance Single flow cache
Flexible NetFlow (FNF)	Template-based flow format (built on V9 protocol) Supports flow monitors (discrete caches) Supports selectable key fields and IPv6 Supports NBAR data fields	Less common Requires more sophisticated platform to produce Requires more sophisticated system to consume
IP Flow Information Export (IPFIX) AKA NetFlow V10	Standardized – RFC 5101, 5102, 6313 Supports variable length fields, NBAR2 Can export flows via IPv4 and IPv6 packets	Even less common Only supported on a few Cisco platforms
NSEL (Cisco ASA only)	Built on NetFlow v9 protocol State-based flow logging (context) Pre and Post NAT reporting	Missing many standard fields Limited support by collectors

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

SFlow

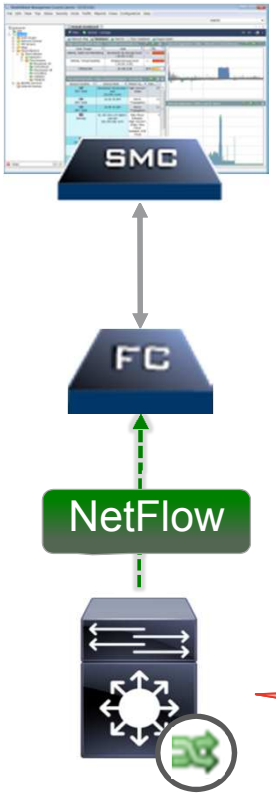
- sFlow
  - Sample-based (packet-sampling) technology
  - RFC-3176
  - Used to monitor high-speed switched networks
  - Samples 1 out of every “n” packets
  - Recommended sample rate = 1/128 packets
  - Duplicate sFlow PDUs must be handled and removed.
  - ***Not recommended for security applications***



© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

Design

NetFlow Deployment Architecture



Management/Reporting Layer:
- Run queries on flow data
- Centralize management and reporting

Flow Collection Layer:
- Collection, storage and analysis of flow records

Flow Exporting Layer:
- Enables telemetry export
- As close to the traffic source as possible

© 2014 Cisco and/or its affiliates. All rights reserved.

NetFlow Deployment

Access:

- New network edge
  - Detect threats as enter the network
- Detect threats inside the switch
  - east-west
  - Layer 2 traffic
- Fewer false positives
  - Higher-granular visibility
- Identify the endpoint
  - collect MAC Address

© 2014 Cisco and/or its affiliates. All rights reserved.

NetFlow Deployment

Distribution & Core:

- Traditional deployment
  - Minimal recommended deployment
- Enable at critical points/bottle necks
- Typically done on a Layer 3 boundary
- Detect threats internal to the VLAN
  - When deployed on an SVI interface
- Detect threats as they traverse the internal network
  - Move between subnets

© 2014 Cisco and/or its affiliates. All rights reserved.

NetFlow Deployment

Edge:

- Detect threats as they enter and leave the network
- Monitor communication between branches
- Gain context from edge devices
  - Application Information
  - Events, NAT & User-ID – NSEL Firewalls

© 2014 Cisco and/or its affiliates. All rights reserved.

Aside: Myths about NetFlow Generation

Myth #1: NetFlow impacts performance

- Hardware implemented NetFlow has no performance impact
- Software implementation is typically significantly <15% processing overhead

Myth #2: NetFlow has bandwidth overhead

- NetFlow is a summary protocol
- Traffic overhead is typically significantly <1% of total traffic per exporting device

© 2014 Cisco and/or its affiliates. All rights reserved.

Components for NetFlow Security Monitoring

Management Console
- Management and reporting

Flow Data

Binary Data Format
– Fast Processing

Flow Collector
- Collect and analyze

Best Practice: Centralize collection globally

Flow Replicator/ UDP Director
- UDP Packet copier
- Forward to multiple collection systems
- Syslog Collector/Repeater

NetFlow

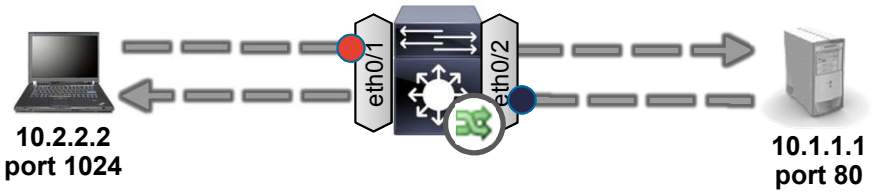
Flow Sensor /Netflow Generation Appliance
- Generate NetFlow data

FlowSensor VE
- Virtual environment

© 2014 Cisco and/or its affiliates. All rights reserved.

NetFlow Collection: Flow Stitching

Uni-directional flow records



Start Time	Interface	Src IP	Src Port	Dest IP	Dest Port	Proto	Pkts Sent	Bytes Sent
10:20:12.221	eth0/1	10.2.2.2	1024	10.1.1.1	80	TCP	5	1025
10:20:12.871	eth0/2	10.1.1.1	80	10.2.2.2	1024	TCP	17	28712

Start Time	Client IP	Client Port	Server IP	Server Port	Proto	Client Bytes	Client Pkts	Server Bytes	Server Pkts	Interfaces
10:20:12.221	10.2.2.2	1024	10.1.1.1	80	TCP	1025	5	28712	17	eth0/1 eth0/2

Bi-directional:

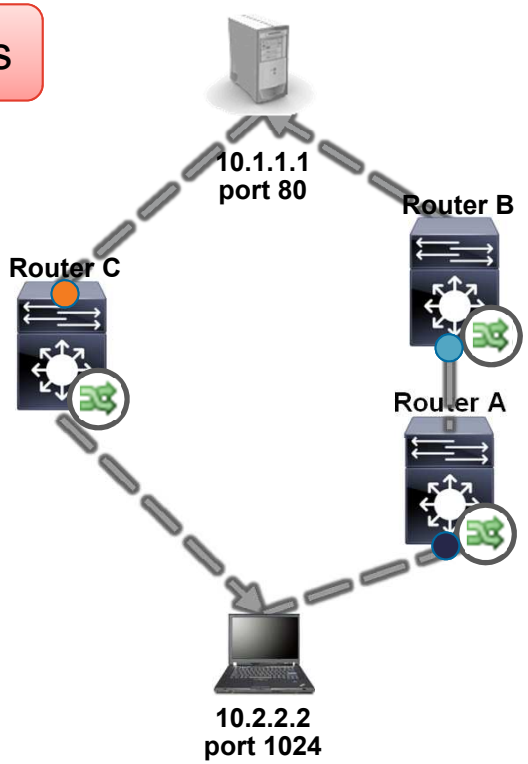
- Conversation flow record
- Allows easy visualization and analysis

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

NetFlow Collection: De-duplication

Duplicates

- Router A: 10.2.2.2:1024 -> 10.1.1.1:80
- Router B: 10.2.2.2:1024 -> 10.1.1.1:80
- Router C: 10.1.1.1:80 -> 10.2.2.2:1024



- Without de-duplication:
  - Traffic volume can be misreported
  - False positive would occur
- Allows for the efficient storage of flow data
- Necessary for accurate host-level reporting
- Does not discard data

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data Center Netflow Design Notes

- Most Data Center Switches do not support full unsampled Netflow – designed for very high speed networks
- Example: only Cisco Nexus 7K M1/M2 Modules support full Netflow in hardware (L2/L3), F-Series Cards (F1, F2, F2E, F3) only support Sampled Netflow
- Cisco Nexus 9K only supports Sflow – sampled only
- **Use Flow Sensor/Netflow Generation Appliances (NGA) on SPAN ports at the Data Center Aggregation Layer.** This also deals with Netflow Cache size issues on these switches (Example: Nexus 7K 512K).

© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Public

Adding Context

Identity Engines as a Telemetry Source

- Maintain historical session table
- Correlate NetFlow to username
- Build User-centric reports

Management Console

Identity Engine

Syslog, REST API

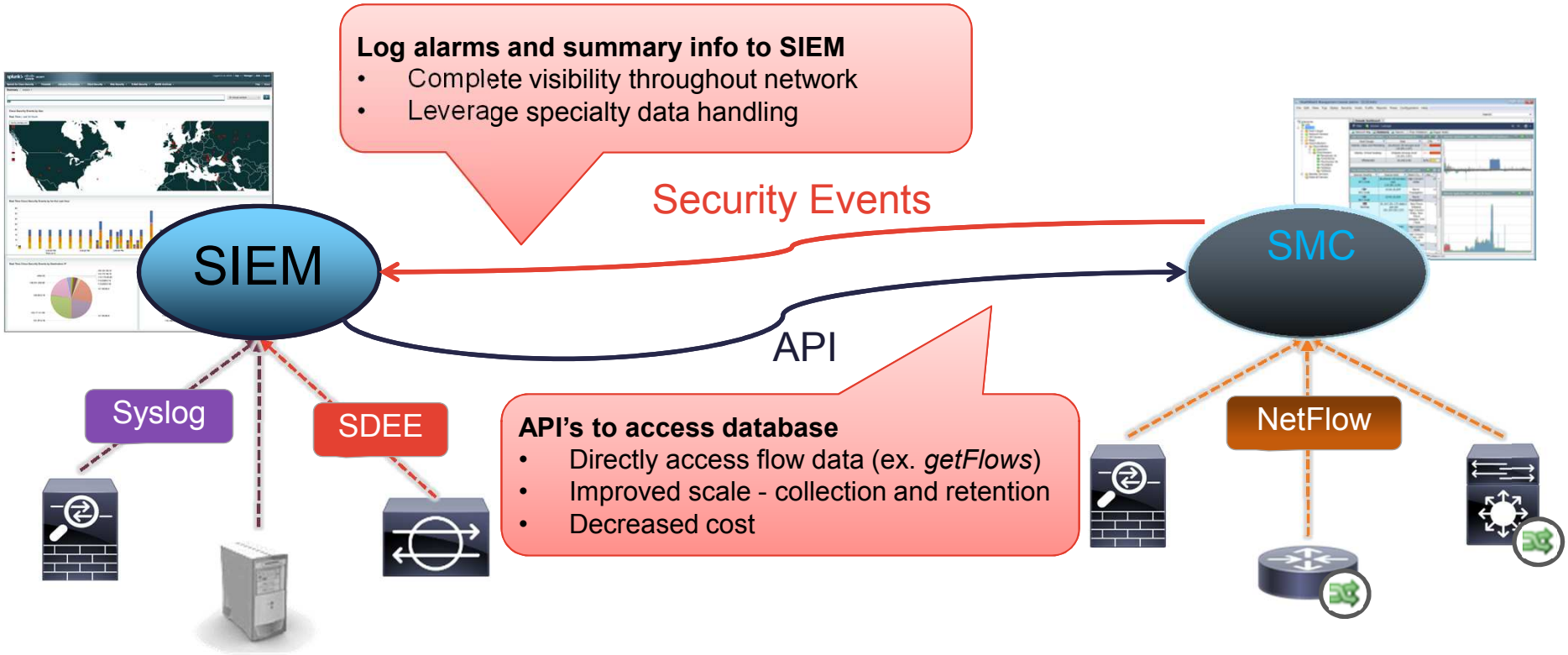
Start Active Time	End Active Ti...	User Name	Host	Device Type	MAC Address
Apr 15, 2013 2:08:33 PM (17 minutes 6s ago)	Current	student01	192.168.103.101	VMWare-Device	00:50:56:85:5c:3d (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	DEMO\student04	192.168.104.100	WindowsXP-Workstation	00:50:56:85:13:c4 (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	host/pod08-mgmt.demo.local	192.168.108.100	WindowsXP-Workstation	00:50:56:85:13:cc (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	host/pod09-mgmt.demo.local	192.168.109.100	WindowsXP-Workstation	00:50:56:85:13:ce (VMware, Inc.)
Apr 15, 2013 2:08:21 PM (17 minutes 18s ago)	Current	DEMO\student05	192.168.105.100	WindowsXP-Workstation	00:50:56:85:13:c6 (VMware, Inc.)

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Apr 15,13 02:08:33.241 PM	✓		student01	00:50:56:85:5C:3D	192.168.103.1...	sw1	GigabitEthernet0/4	PermitAccess
Apr 15,13 02:08:21.241 PM	✓		DEMO\student04	00:50:56:85:13:C4	192.168.104.1...	sw1	GigabitEthernet0/5	PermitAccess
Apr 15,13 02:08:21.219 PM	✓		host/pod08-mgmt.demo.local	00:50:56:85:13:CC	192.168.108.1...	sw1	GigabitEthernet0/9	PermitAccess
Apr 15,13 02:08:21.192 PM	✓		host/pod09-mgmt.demo.local	00:50:56:85:13:CE	192.168.109.1...	sw1	GigabitEthernet0/10	PermitAccess
Apr 15,13 02:08:21.144 PM	✓		DEMO\student05	00:50:56:85:13:C6	192.168.105.1...	sw1	GigabitEthernet0/6	PermitAccess
Apr 15,13 02:08:21.082 PM	✓		DEMO\stu...	00:50:56:85:13:CA	192.168.107.1...	sw1	GigabitEthernet0/8	PermitAccess

Authenticated Session Table

© 2014 Cisco and/or its affiliates. All rights reserved.

Integrating with a SIEM



© 2014 Cisco and/or its affiliates. All rights reserved.

Netflow for Security – Vertical Focus

- Focus on verticals that truly care about APT threats: Financials, Utilities, Government, High Tech, Pharma
- If you are a customer that is not or does not have fully deployed traditional defenses such as NGFW, NGIPS, Web Security, and others then focus on these

© 2014 Cisco and/or its affiliates. All rights reserved.