



全方位的安全保护 StealthWatch 解决方案介绍

Song Li

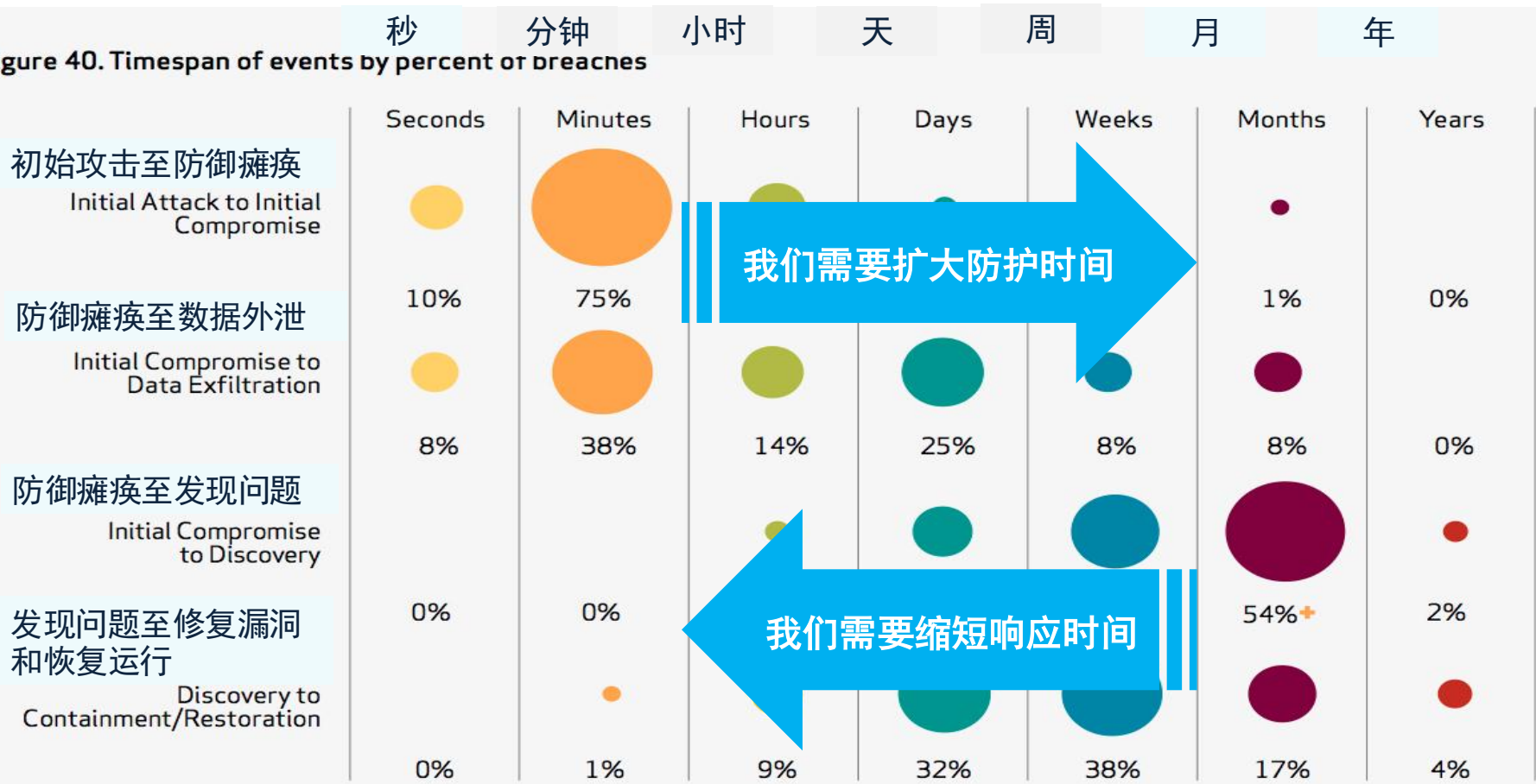
安全顾问工程师

日程

- 思科网络安全战略
- StealthWatch解决方案介绍

我们客户目前遇到的问题？

Figure 40. Timespan of events by percent of breaches

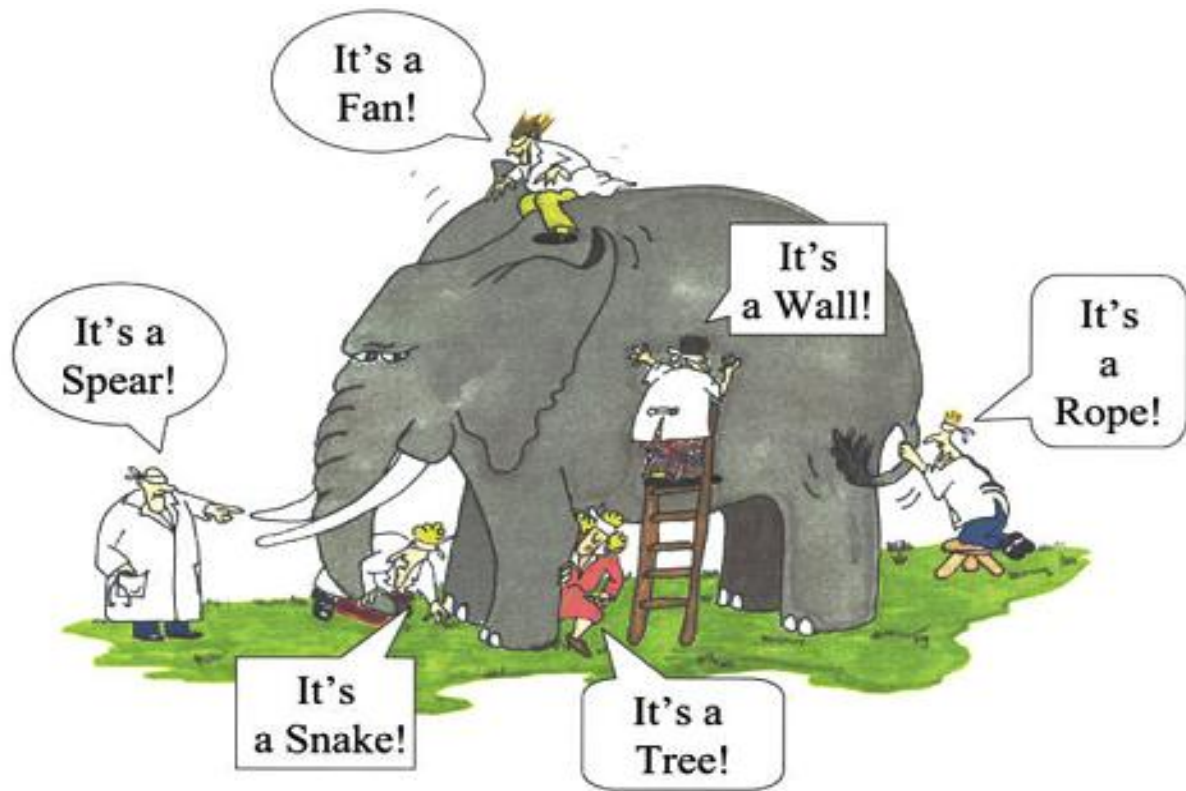


我们需要扩大防护时间

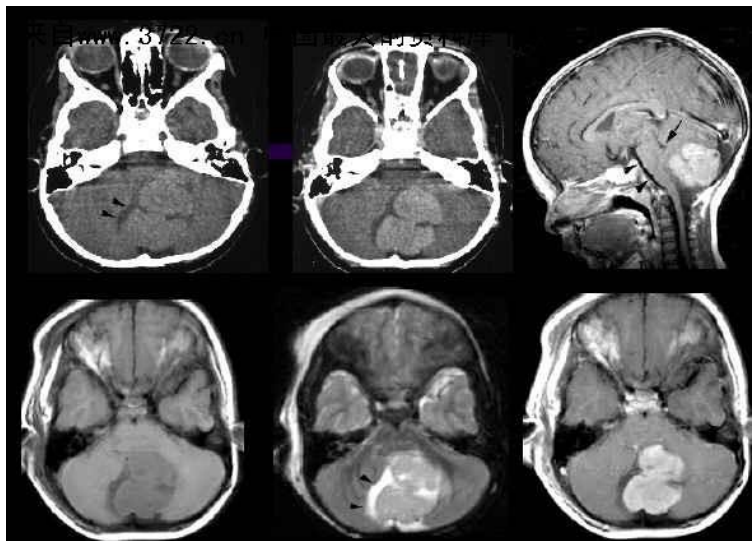
我们需要缩短响应时间

来源：《2012年Verizon数据泄露调查报告》

安全设备一个不少 但遇到安全问题…….



对于威胁 应该基于特征还是行为



望
王
聞
切

网络基础平台其实可以为安全做出更多



细粒度隔离



减少横向移动
加强动态细粒度控制，
合规

网络作为传感器



监测异常信息流
恶意设备及应用，以及用户的
使用违规现象

快速缓解



自动隔离
流量重定向
实时应用控制

思科动态防御模型——解决安全难题



思科方案助力用户解决安全难题

全面提高可见性 Visibility-Driven



与网络设备集成，
情景感知
自动化
提供安全防护的准确依据



网络

真正解决用户面临的威胁 Threat-Focused



高级威胁防御
云安全智能
减少恶意威胁造成的损失



终端



移动



虚拟化

统一平台实现整体安全防护 Platform-Based



灵活开放平台，
可扩展，全面控制与管理
提供统一动态的安全防护



云

日程

- 思科网络安全战略
- StealthWatch解决方案介绍

你不能保护你不能看到的！

60% 的数据在小时之内
就可以被盗取

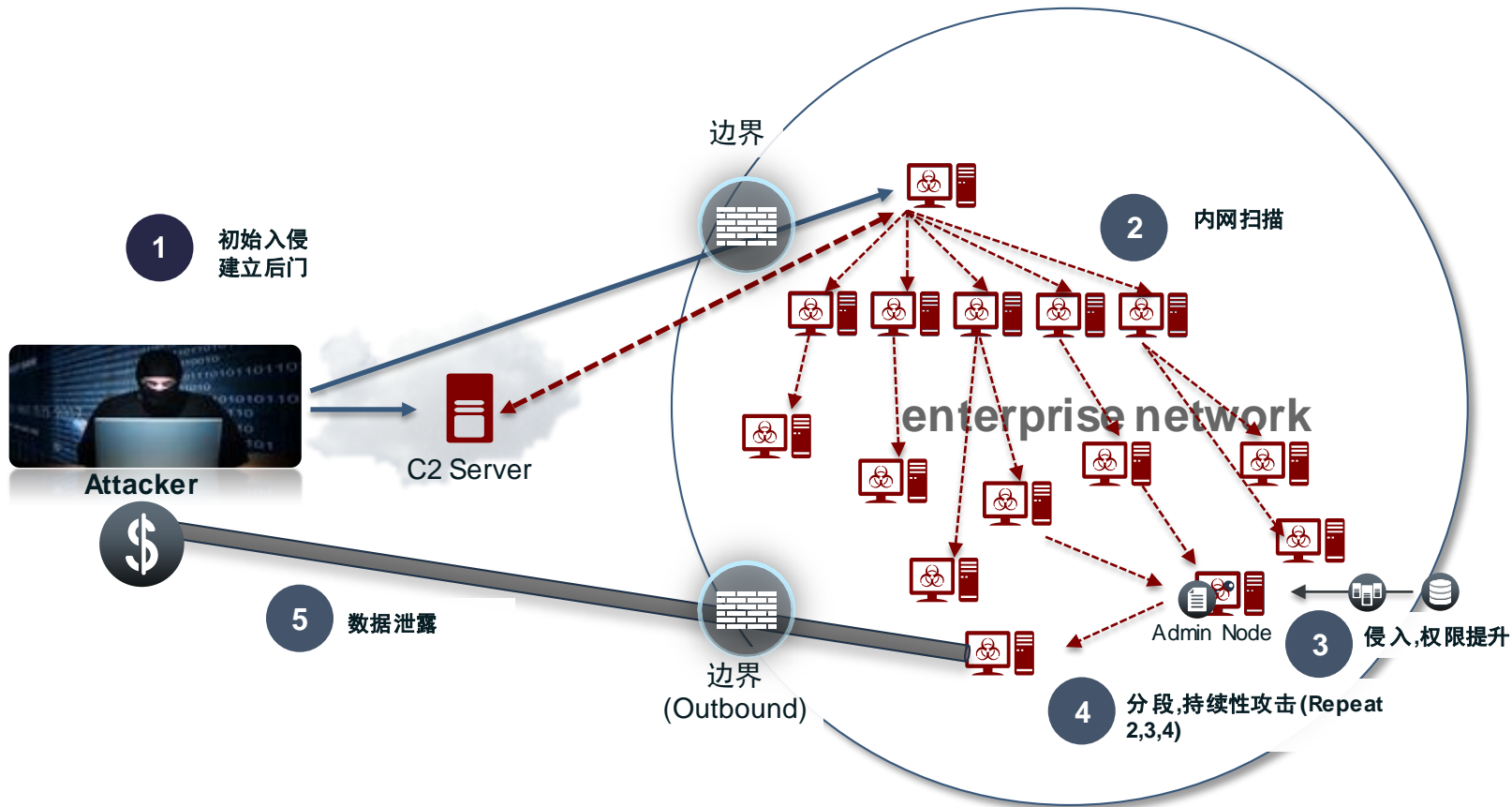
85% 的安全事件是在几周之内才
被发现

54% 的黑客留有的后门再数
月才被检测到

51%

的公司在过去3年
内由于安全事件造
成百万资产的损失

如今的环境中 网络是否还有边界



思科CTD解决方案-差异化价值



采样法 = 部分监控

- 部分流量 (不超过 5%)
- 对现有网络给出流量快照
- 仅对一本书的头200个词进行阅读



非采样法 = 监控全部

- 所有网络流量都将被查看
- 监控所有实时流量
- 确保一本书的全部内容被阅读

采样方式对于网络性能监控是可行的，但对比安全并不是很好的建议!!!

利用网络获得最大的可见性和可控性

检测异常流量

检测用户网络访问滥用

获得网络全面可见性

Network As A
Sensor (NaaS)



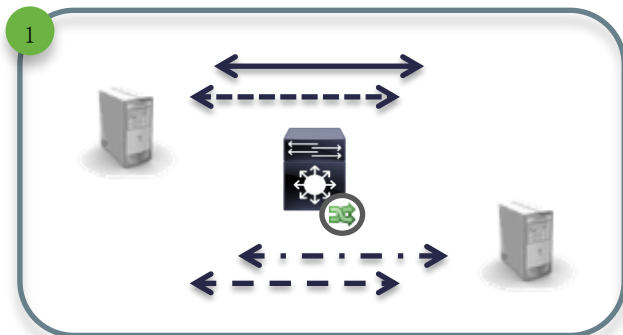
Network As An
Enforcer
(NaaE)

动态隔离, 抑制攻击

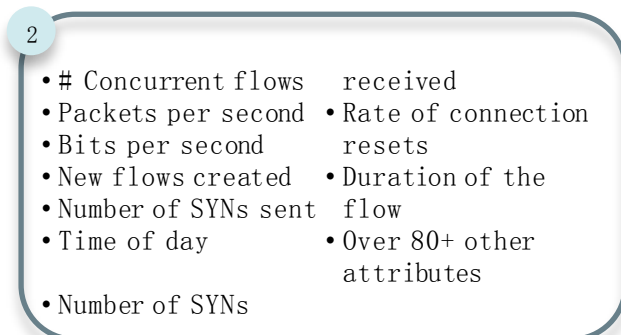
对核心资产部署访问控制

动态的策略/用户组

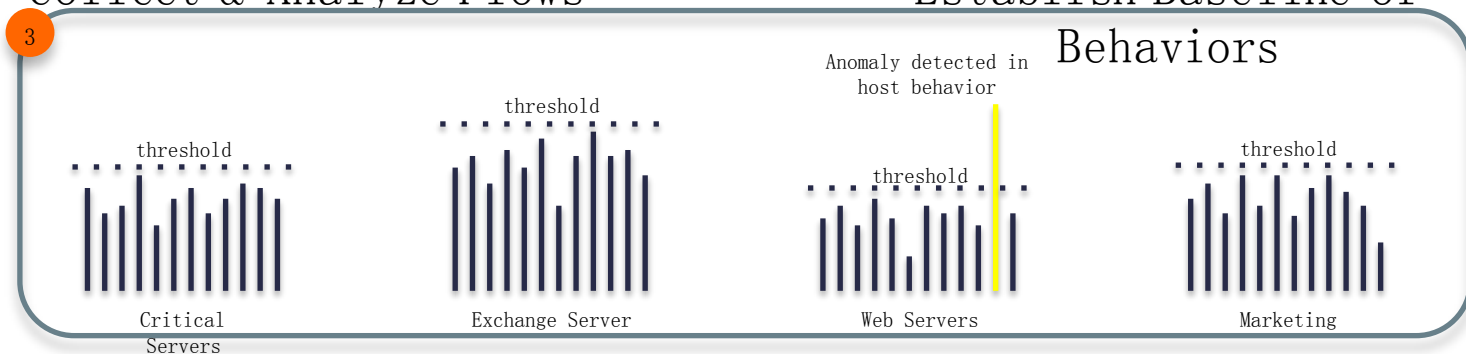
利用基于行为的异常检测——检测高级威胁



Collect & Analyze Flows

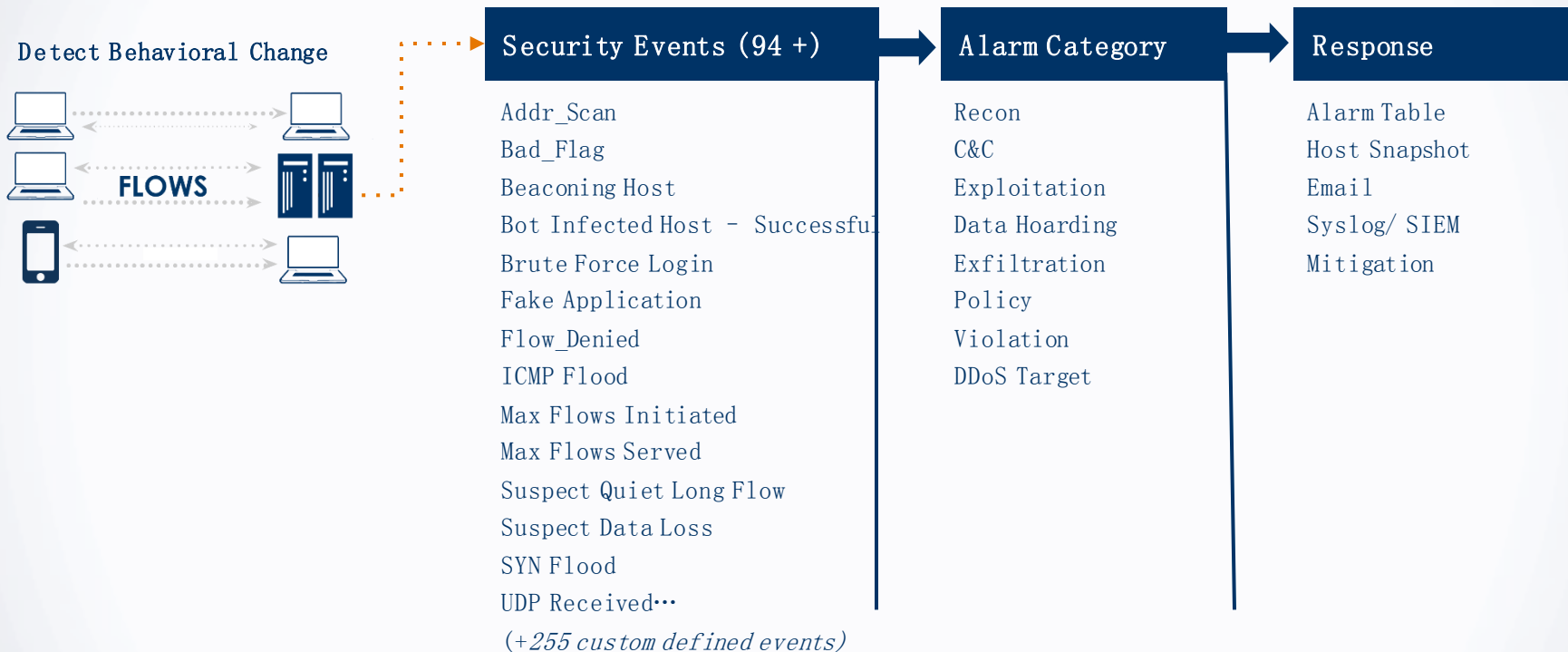


Establish Baseline of Behaviors



Alarm on Anomalies & Changes in Behavior

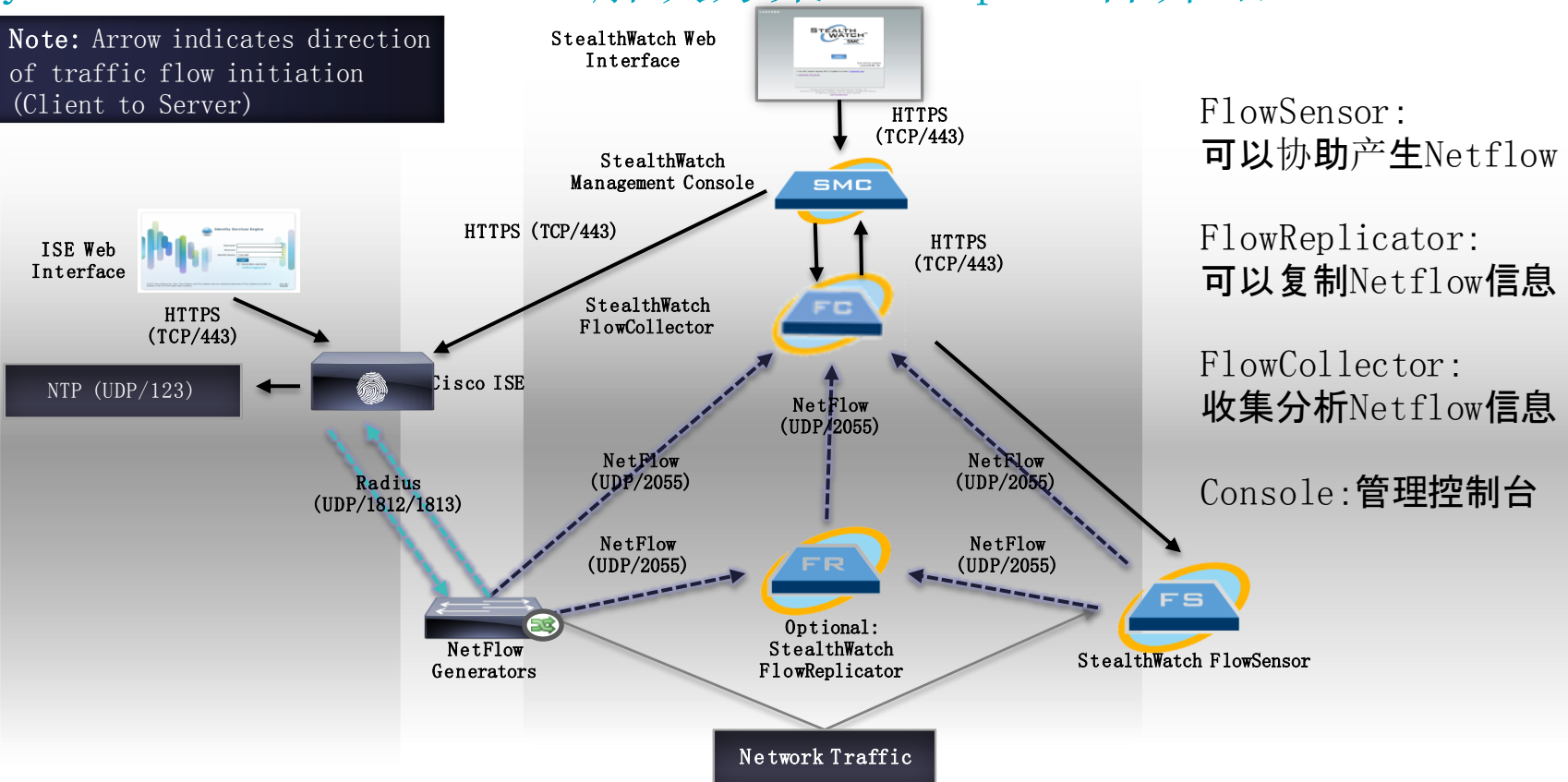
行为检测模式



数据流被采集后，通过行为分析算法来发现并建立“安全事件”。 “安全事件”将会通过“加点”方式来归类到一个告警类，这样非常容易且高准确率检测到可以行为。

Cyber Threat Defense 解决方案Lancope组件介绍

Note: Arrow indicates direction of traffic flow initiation (Client to Server)



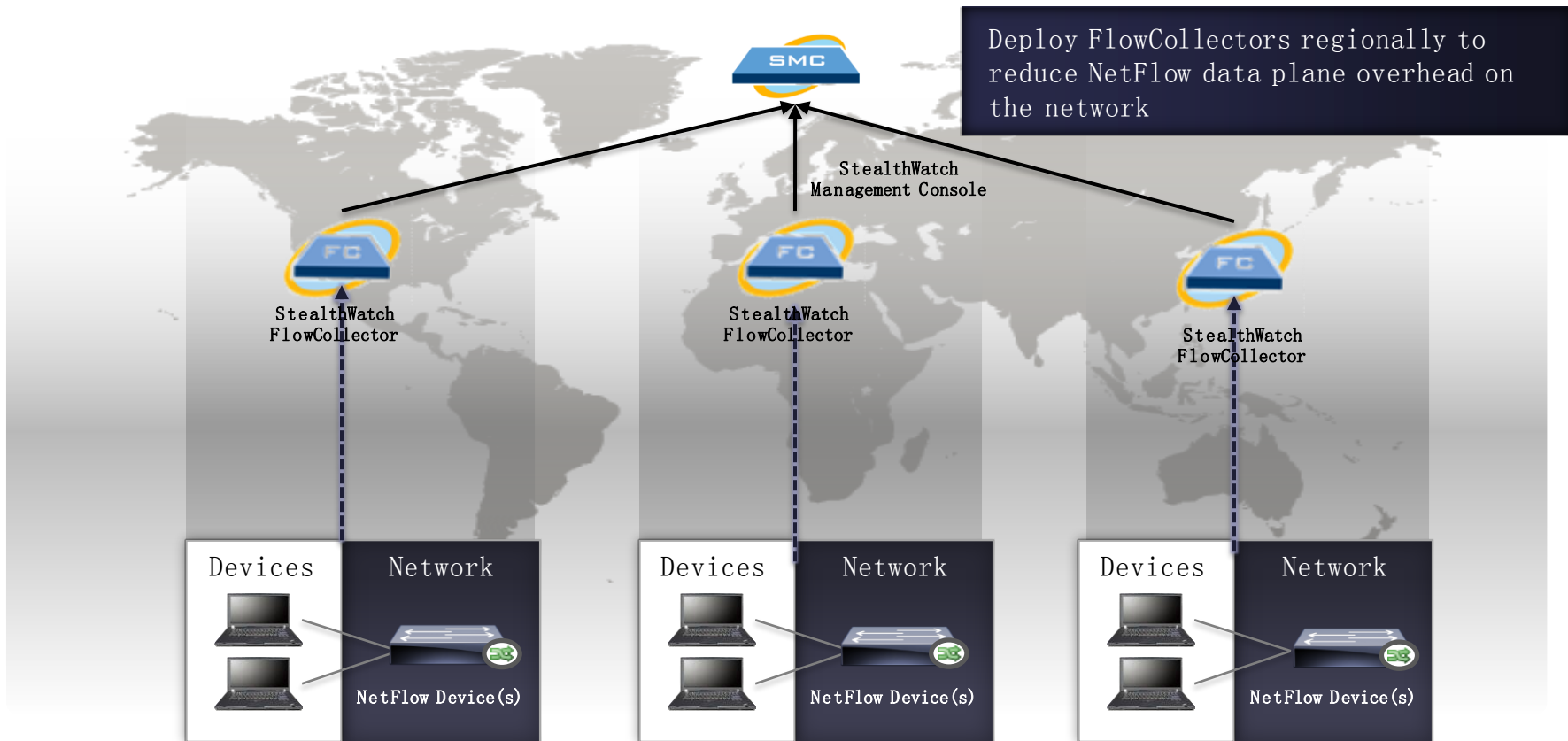
FlowSensor:
可以协助产生Netflow

FlowReplicator:
可以复制Netflow信息

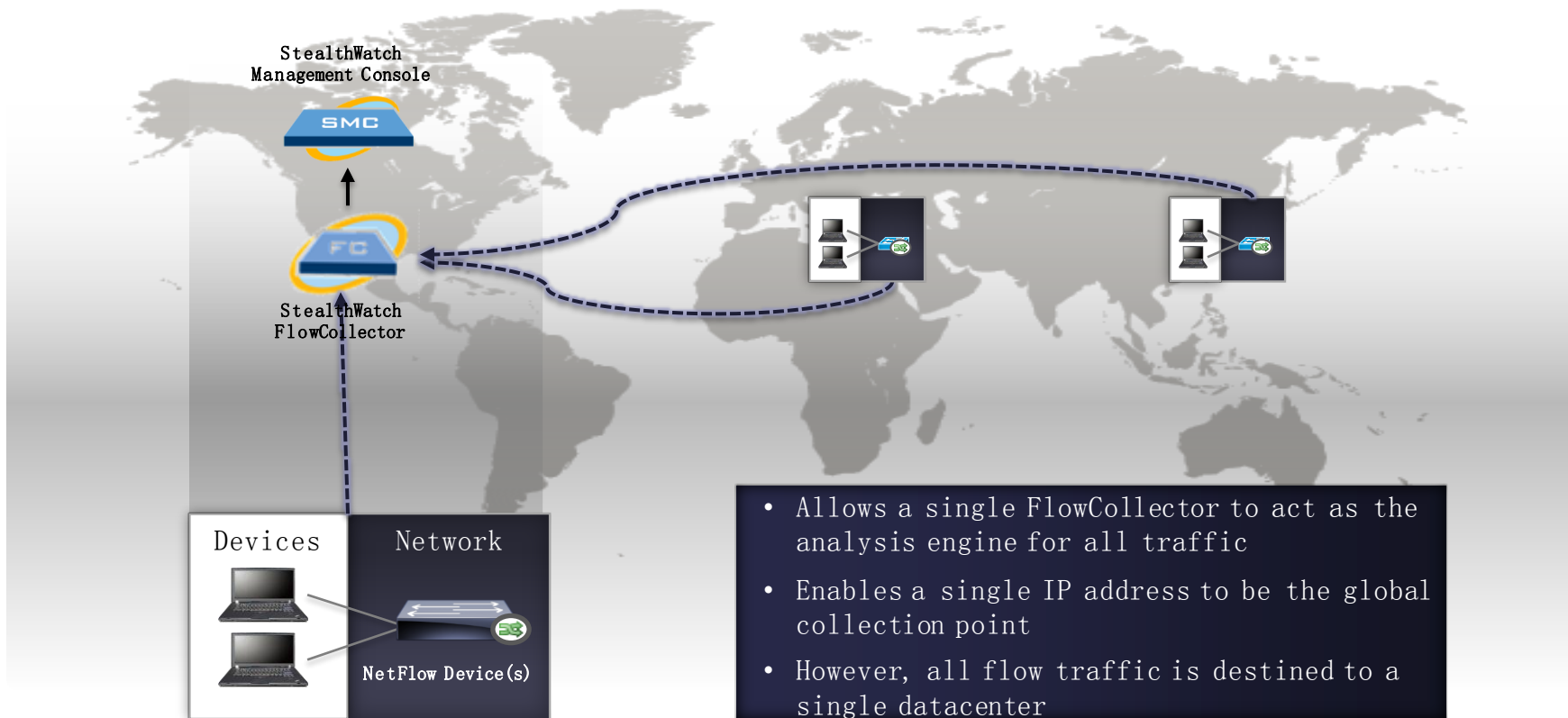
FlowCollector:
收集分析Netflow信息

Console: 管理控制台

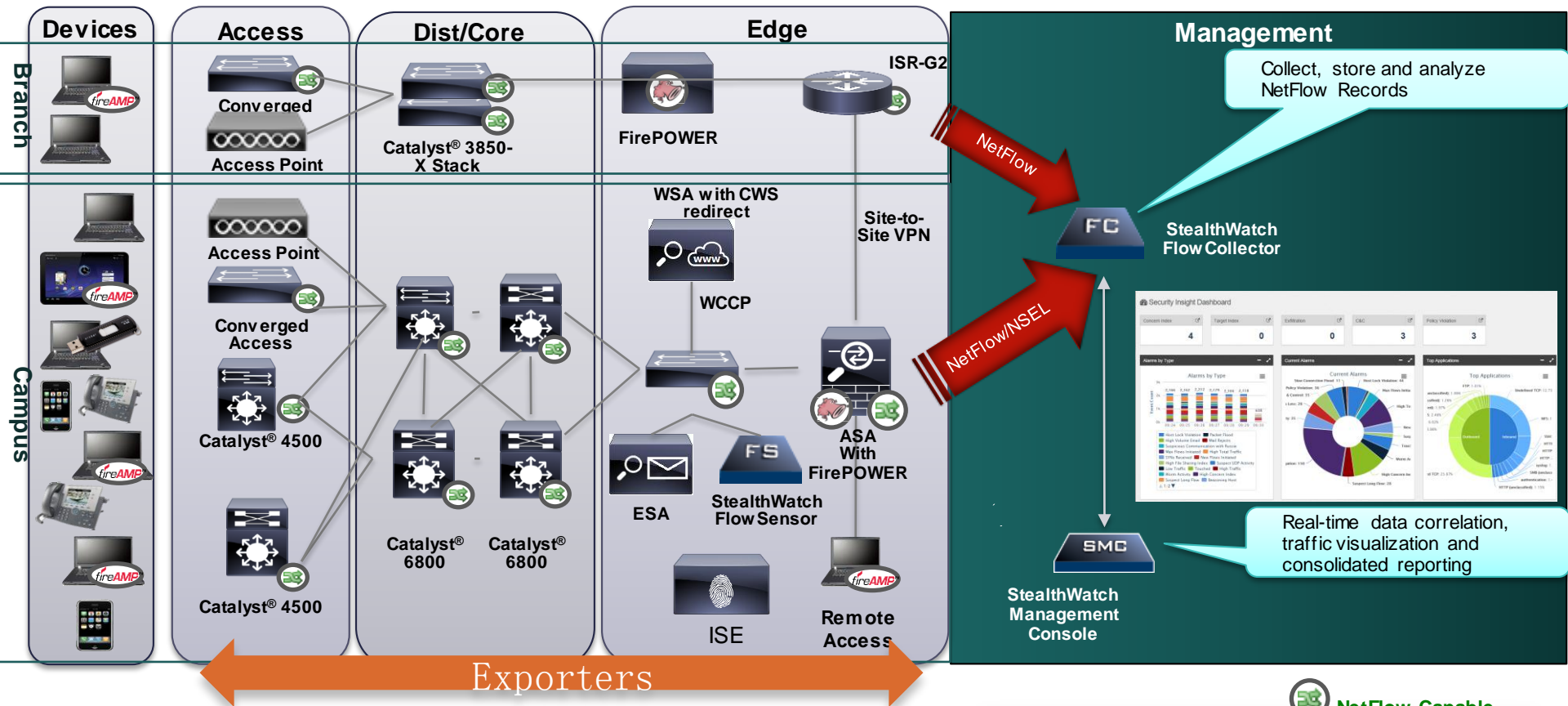
FlowCollector 部署 - 分布式部署



FlowCollector 部署 - 集中式

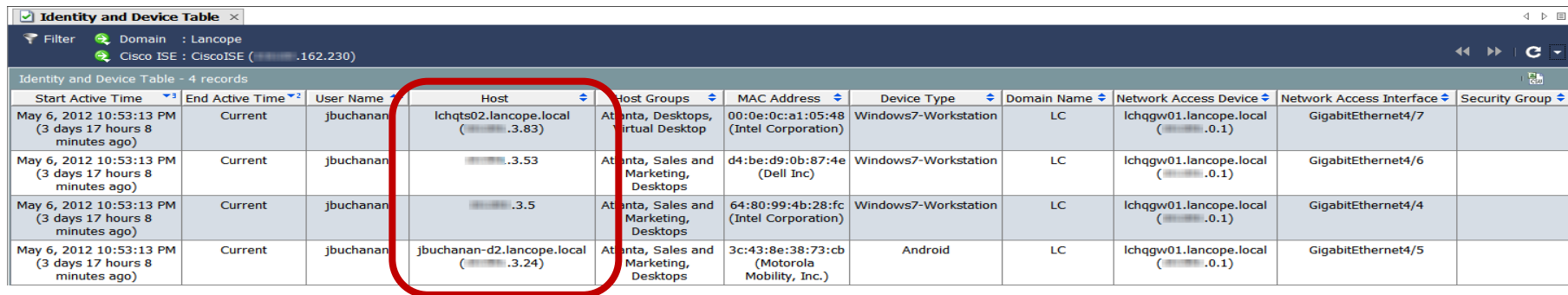


StealthWatch 解决方案架构



案例: 如何解决网速慢

- Network slow
 - 通过用户找到对应IP地址.



Identity and Device Table - 4 records

Start Active Time	End Active Time	User Name	Host	Host Groups	MAC Address	Device Type	Domain Name	Network Access Device	Network Access Interface	Security Group
May 6, 2012 10:53:13 PM (3 days 17 hours 8 minutes ago)	Current	jbuchanan	lchqts02.lancope.local (.3.83)	Atlanta, Desktops, Virtual Desktop	00:0e:0c:a1:05:48 (Intel Corporation)	Windows7-Workstation	LC	lchqgw01.lancope.local (.0.1)	GigabitEthernet4/7	
May 6, 2012 10:53:13 PM (3 days 17 hours 8 minutes ago)	Current	jbuchanan	.3.53	Atlanta, Sales and Marketing, Desktops	d4:be:d9:0b:87:4e (Dell Inc)	Windows7-Workstation	LC	lchqgw01.lancope.local (.0.1)	GigabitEthernet4/6	
May 6, 2012 10:53:13 PM (3 days 17 hours 8 minutes ago)	Current	jbuchanan	.3.5	Atlanta, Sales and Marketing, Desktops	64:80:99:4b:28:fc (Intel Corporation)	Windows7-Workstation	LC	lchqgw01.lancope.local (.0.1)	GigabitEthernet4/4	
May 6, 2012 10:53:13 PM (3 days 17 hours 8 minutes ago)	Current	jbuchanan	jbuchanan-d2.lancope.local (.3.24)	Atlanta, Sales and Marketing, Desktops	3c:43:8e:38:73:cb (Motorola Mobility, Inc.)	Android	LC	lchqgw01.lancope.local (.0.1)	GigabitEthernet4/5	

Best Practices – Analyzing Flows

- Network slow
 - 查看接口是否有流量过载

Identity and Device Table x [redacted].3.83 x

Filter Domain : Lancope Time : Today
Host : [redacted].3.83

Identification Alarms Security CI Events Top Active Flows Identity, DHCP & Host Notes **Exporter Interfaces**

Closest Interfaces - 1 record

Appliance	Exporter	Interface	Description	Confidence (%)
FlowCollector01 ([redacted].0.40)	lchqgw01.lancope.local ([redacted].0.1)	Vlan1	Desktops	100

Interfaces Seeing This Host as a Source in Active Flows - 6 records

Exporter	Exporter Type	Interface	Direction	Current Utilization	Current Traffic (bps)
FlowSensor-Ninjanet ([redacted].3.112)	FlowSensor	eth3	Inbound	0.61% <input type="text"/>	6.12M
FlowSensor-Core01 ([redacted].1.163)	FlowSensor	eth3	Inbound	0.55% <input type="text"/>	5.5M
lchqgw01.lancope.local ([redacted].0.1)	Exporter	Vlan1	Outbound	0.44% <input type="text"/>	4.37M
lchqgw01.lancope.local ([redacted].0.1)	Exporter	Vlan1	Inbound	0.25% <input type="text"/>	2.46M

Interfaces Seeing This Host as a Destination in Active Flows - 8 records

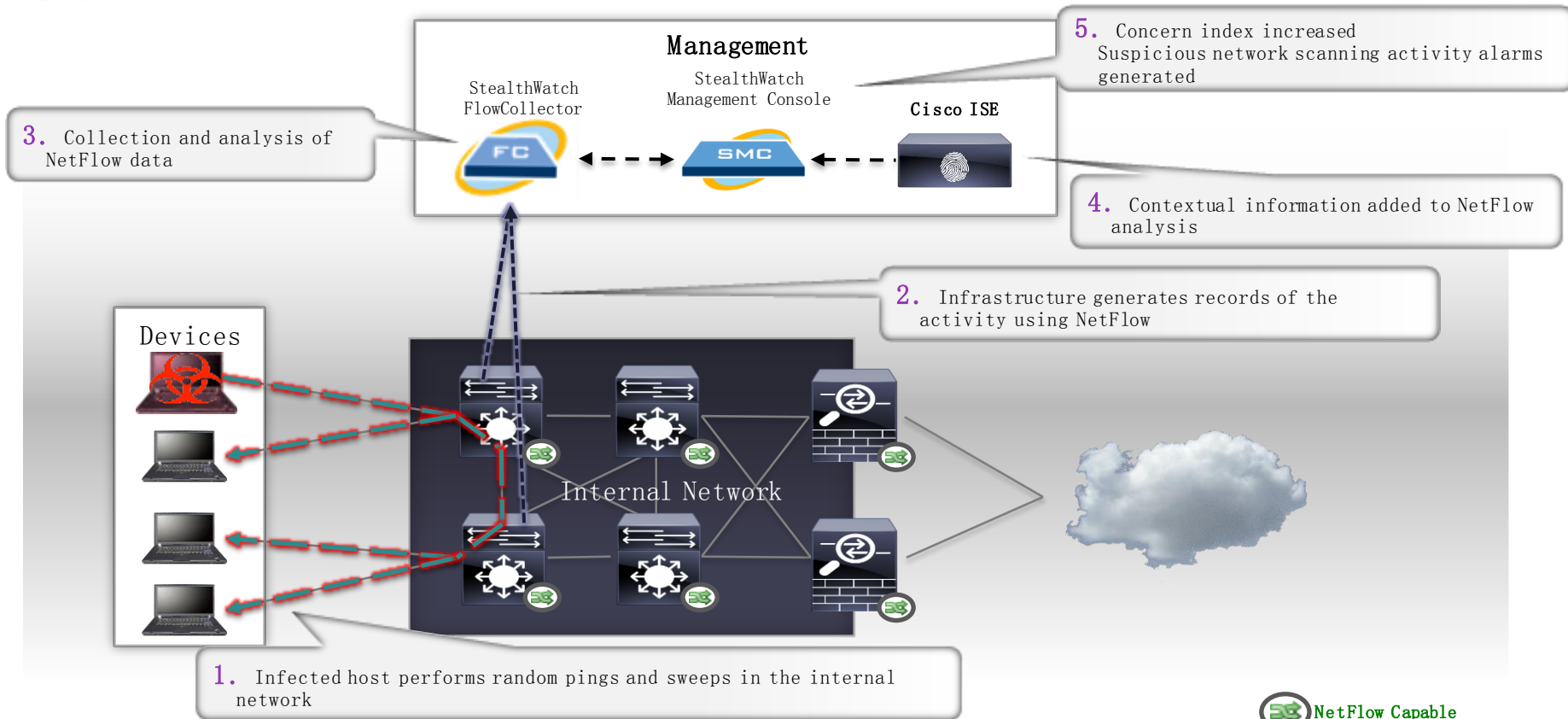
Exporter	Exporter Type	Interface	Direction	Current Utilization	Current Traffic (bps)
lchqgw01.lancope.local ([redacted].0.1)	Exporter	Vlan202	Outbound	0.83% <input type="text"/>	8.33M
FlowSensor-Ninjanet ([redacted].3.112)	FlowSensor	eth3	Inbound	0.61% <input type="text"/>	6.12M
FlowSensor-Core01 ([redacted].1.163)	FlowSensor	eth3	Inbound	0.55% <input type="text"/>	5.5M
lchqgw01.lancope.local ([redacted].0.1)	Exporter	Vlan1	Outbound	0.44% <input type="text"/>	4.37M

Best Practices – Analyzing Flows

- Network slow
 - 如果没有接口流量过载, 查看Top Active Flows.
 - High SRT (Server Response Time) = Server Issue
 - High RTT (Round Trip Time)= Network/Host Issue

Start Active Time	This H...	Connected To	Connected ...	Protocol	Service	Bytes Out...	Bytes In...	Average ...	RTT Average	SRT Average
Feb 22, 2012 11:18:24 AM (1 minute 21s ago)	Client	0.23	Atlanta	tcp	http	6.55k	26.17k	134.0k	1ms	1ms
Feb 17, 2012 8:44:50 AM (5 days 2 hours 34 minutes ago)	Client	162.230	SG Public, BC Webserver	tcp	https	57.72M	2.49G	49.56k	1ms	1ms
Feb 22, 2012 11:16:52 AM (2 minutes 53s ago)	Client	74.83	United States	tcp	http	80.43k	248.2k	28.95k	4ms	2ms
Feb 22, 2012 11:18:29 AM (1 minute 16s ago)	Client	234.66	United States	tcp	http	964	1.85k	22.85k	80ms	371ms
Feb 22, 2012 11:16:52 AM (2 minutes 53s ago)	Client	162.8	United States	tcp	http	47.21k	31.33k	6.92k	5ms	2ms
Feb 22, 2012 11:18:29 AM (1 minute 16s ago)	Client	237.212	United States	tcp	http	2.15k	3.13k	3.94k	18ms	1ms
Feb 17, 2012 8:45:00 AM (5 days 2 hours 34 minutes ago)	Client	13.133	United States	tcp	http	134.62M	37.89M	3.28k	23ms	3ms
Feb 22, 2012 11:17:04 AM	Client	3.35	United States	tcp	http	9.75k	18.56k	2.86k		

案例: 识别网络扫描行为



识别扫描行为

Concern Index Table

High Concern Index indicates a significant number of suspicious events

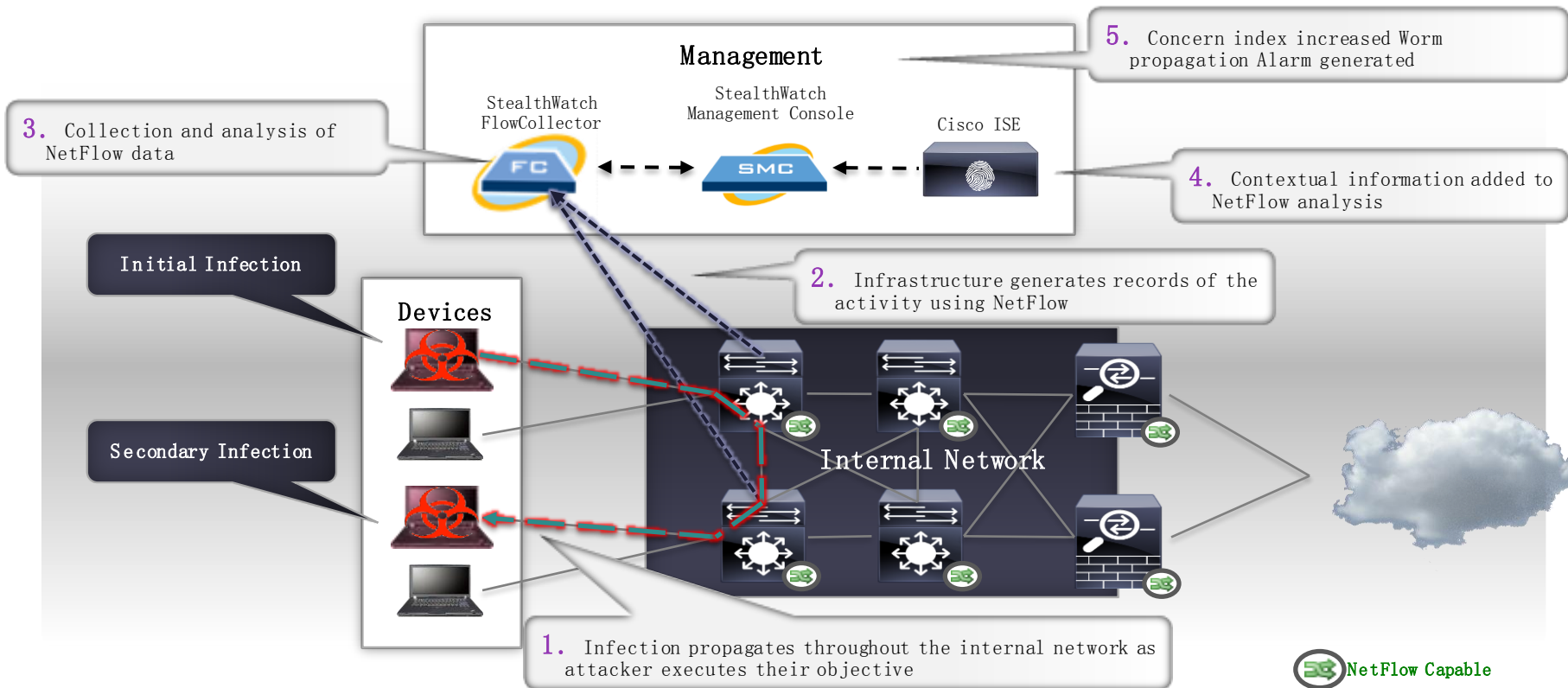
Suspicious network scanning activity

Summary - 9 records summarized into 9 records

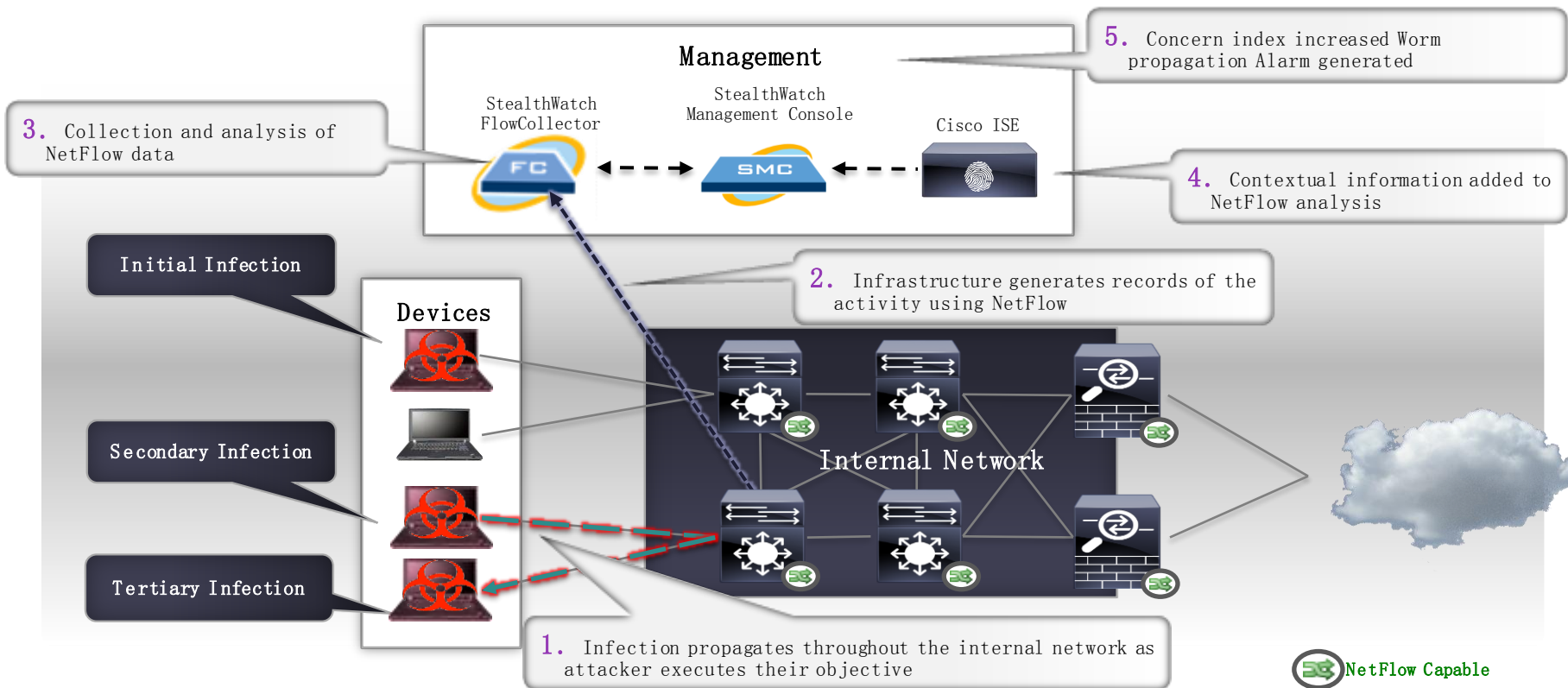
Host Groups	Host	CI	CI%	Alarms	Alerts
Desktops, Internal 3rd Party Managed Devices, By Location, Trusted Internet Hosts, Flickr	10.201.3.23	338,137,280	112.712%		Ping_Oversized_Packet
SMS Servers, External IPs, By Location, Flickr	(209.182.184.2)	103,869,936	1.039%		Excess_Clients, Excess_Servers, Ping_Rejects, Spoof, TCP_Scan, UDP_Scan
WebEx.com, By Function, By Location, Trusted Internet Hosts, Flickr	10.202.1.122	2,328,268	776%	High Concern Index, ICMP Flood	Ping_Oversized_Packet, Rejects
Firewalls, By Location, PGP Corp, Trusted Internet Hosts, Flickr	(10.192.0.1)	10,875,454	109%	High Concern Index	Ping, Ping_Oversized_Packet, Ping_Scan
Application Servers, By Location, Flickr	209.182.176.42	2,539,292	79%		Rejects, Spoof
WebEx.com, By Function, By Location, Trusted Internet Hosts, Flickr	(10.202.1.70)	1,083,341	76%		Rejects, UDP_Scan
Desktops, By Location, Trusted Internet Hosts, Flickr	(10.10.10.10)	409,118	75%		Rejects, UDP_Scan
Servers, Atlanta, Internal 3rd Party Managed Devices, Trusted Internet Hosts, Flickr	(10.201.0.1)	188,988	63%	Suspect UDP Activity	Rejects, UDP_Scan
By Location, PGP Corp, Trusted Internet Hosts, Flickr	(10.192.0.58)	186,579	62%		UDP_Scan

IP Address/DNS name

案例:检测内部恶意软件传播



检测内部恶意软件传播



检测内部恶意软件传播

The screenshot shows a network security interface with the following details:

- Filter: Domain: [redacted], Host: 10.40.10.254, Time: February 1, 2012
- Alarms: 1 record
- Appliance: FlowCollector01 (10.192.0.192)
- Severity: Critical
- Count: 5(0)

Start Active Time	Alarm	Source	Details
Feb 1, 2012 8:39:30 PM (12 days 19 hours 27 minutes ago)	Worm Propagation	10.40.10.254	Worm propagated from Source Host using ms-rpc (135/tcp) (Double-click for details)
Feb 1, 2012 7:40:00 PM (12 days 20 hours 26 minutes ago)	New Flows Initiated	10.40.10.254	Observed 1.07k flows. Policy maximum allows up to 1k flows.
Feb 1, 2012 7:39:30 PM (12 days 20 hours 27 minutes ago)	Worm Propagation	10.40.10.254	Worm propagated from Source Host using ms-rpc (135/tcp) (Double-click for details)
Feb 1, 2012 6:40:00 PM (12 days 21 hours 26 minutes ago)	New Flows Initiated	10.40.10.254	Observed 1.12k flows. Policy maximum allows up to 1k flows.
Feb 1, 2012 6:39:30 PM (12 days 21 hours 27 minutes ago)	Worm Propagation	10.40.10.254	Worm propagated from Source Host using ms-rpc (135/tcp) (Double-click for details)
Feb 1, 2012 5:40:00 PM (12 days 22 hours 26 minutes ago)	New Flows Initiated	10.40.10.254	Observed 1.04k flows. Policy maximum allows up to 1k flows.

IP Address

Alarm indicating this host touched another host which then began exhibiting the same suspicious behavior

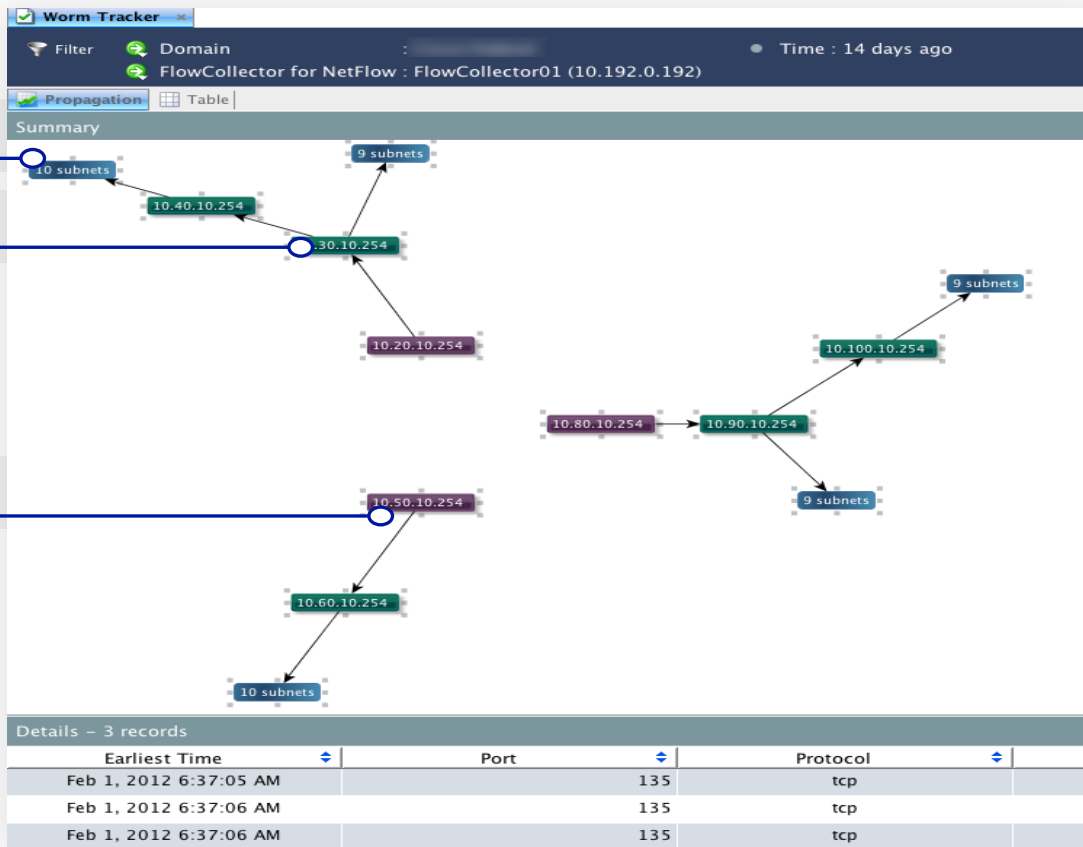
Suspicious activity that triggered the alarm

感染轨迹

第三感染

第二个感染

初始感染



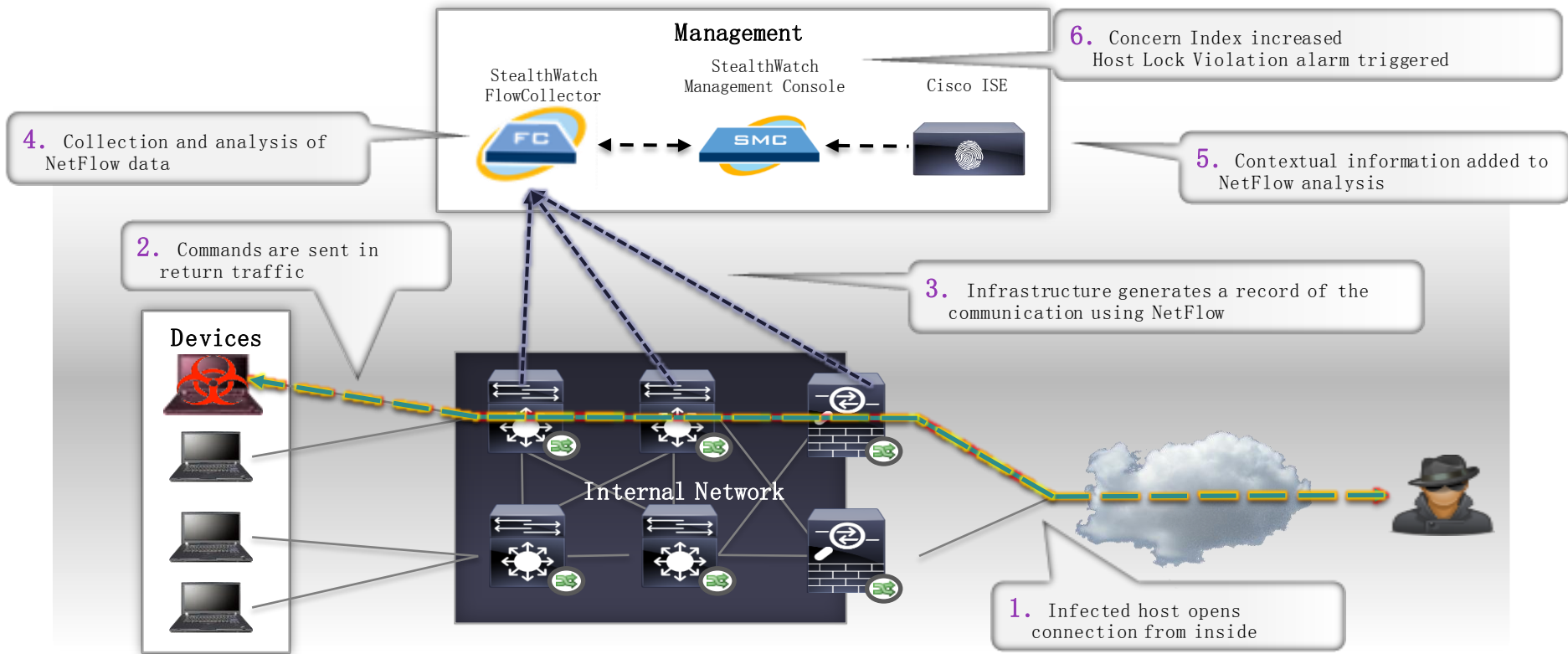
检测内部恶意软件传播

超过100种以上的检测算法

Country	Host	CI	Alerts	Client Services
United States	70.46.194.122.nv.nu vox.net	28,545,681	Excess_Clients, Long_Ping, New_Host, Ping, Ping_Scan, Rejects, TCP_Scan	VMware-client, auth, bgp, dnstcp, finger, ftp, h323, http, http-alt, https, imap4, ipp, isakmp, kerberos, ms-rpc, ncp, netbios-ss, nntp, pop, pop3s, rtsp, samba-web, slp, smb, smtp, ssh, tacacs, telnet, time, unix-rpc, whois, wins, 17/tcp, 30/tcp, 199/tcp, 256/tcp
United States	10-234-115-208.rev erse.lstn.net	7,226,510	Excess_Clients, TCP_Scan	icq, kazaa, mc-client, ms-rpc, rat, socks, 1032/tcp, 1034/tcp, 1036/tcp, 1042/tcp
Germany	a81-14-226-150.net -htp.de	2,362,728	TCP_Scan	smb
Korea, Republic Of	183.110.241.106	2,131,262	Excess_Clients, TCP_Scan	UPnP, bittorrent, dc++, finger, h323, http, ipp, irc, macromedia, ms-olap, ms-sms, msn-im, mysql, netmeeting, postgresql, remote-desktop, rsync, smtp, vnc, wbem, xwindows, 655/tcp, 730/tcp, 1044/tcp, 3339/tcp
China	86.12.142.61.broad.d g.gd.dynamic.163data .com.cn	1,919,609	UDP_Scan	sql-server
China	211.143.23.132	1,908,593	UDP_Scan	sql-server
China	211.141.79.26	31,052	UDP_Scan	sql-server
China	61.160.107.254	12,035	Ping_Scan	
China	58.221.28.142	9,018	New_Host, TCP_Scan	6239/tcp, 14433/tcp, 18530/tcp, 22627/tcp

- Addr_Scan/tcp
- Addr_Scan/udp
- App_Fake/tcp
- App_Fake/udp
- Bad_Flag_ACK
- Bad_Flag_All
- Bad_Flag_NoFlg
- Bad_Flag_Rsrvd
- Bad_Flag_RST
- Bad_Flag_SYN_FIN
- Bad_Flag_URG
- Bad_Flags
- Frag:First_Too_Short
- Frag:Packet_Too_Long
- Frag:Sizes_Differ
- Half_Open_Attack
- ICMP_Comm_Admin
- ICMP_Dest_Host_Admin
- ICMP_Dest_Host_Unk
- ICMP_Dest_Net_Admin
- ICMP_Dest_Net_Unk
- ICMP_Flood
- ICMP_Frag_Needed
- ICMP_Host_Precedence
- ICMP_Host_Unreach
- ICMP_Host_Unreach_TOS
- ICMP_Net_Unreach
- ICMP_Net_Unreach_TOS
- ICMP_Port_Unreach
- ICMP_Precedence_Cutoff
- ICMP_Proto_Unreach
- ICMP_Src_Host_Isolated

案例:检测命令控制 (CnC) 通道



检测命令与控制（CnC）通道

Alarm indicating communication with known BotNet Controllers

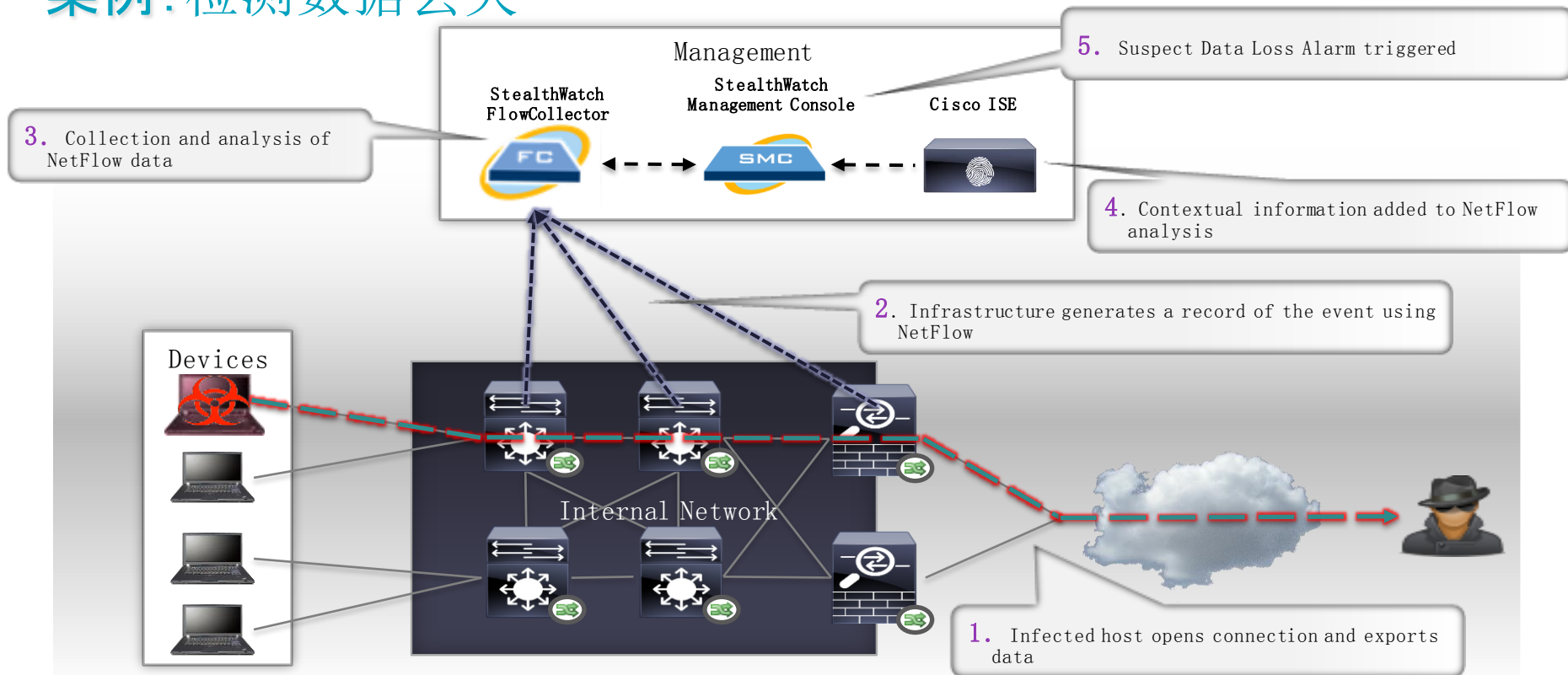
IP Address

Source user name

Policy that triggered alarm

Policy	Start Active Time	Alarm	Source	Source Host Groups	Source User	Target	Target Host	Details
Inside Hosts	Jan 27, 2012 3:29:00 PM (8 minutes 10s ago)	Host Lock Violation	10.35.88.171	Remote VPN IP Pool			Zeus Botnet Controllers, United States	Rule #1 Suspicious Hosts Flow TO Source Host is using https (443/tcp) as client to pw-in-f104.1e100.net (Double-click for details)
Inside Hosts	Jan 27, 2012 3:32:00 PM (5 minutes 10s ago)	Host Lock Violation	10.34.85.19	Catch All			Zeus Botnet Controllers, United States	Rule #1 Suspicious Hosts Flow TO Source Host is using http (80/tcp) as client to pz-in-f102.1e100.net (Double-click for details)
Inside Hosts	Jan 27, 2012 3:34:30 PM (2 minutes 40s ago)	Host Lock Violation	10.34.85.20	Catch All			Zeus Botnet Controllers, United States	Rule #1 Suspicious Hosts Flow TO Source Host is using https (443/tcp) as client to pz-in-f99.1e100.net (Double-click for details)
Inside Hosts	Jan 27, 2012 3:35:30 PM (1 minute 40s ago)	Host Lock Violation	10.34.85.20	Catch All			Zeus Botnet Controllers, United States	Rule #1 Suspicious Hosts Flow TO Source Host is using http (80/tcp) as client to nuq04s06-in-f1.1e100.net (Double-click for details)
Inside Hosts	Jan 27, 2012 3:37:00 PM (10s ago)	Host Lock Violation	10.34.77.154	Catch All			Zeus Botnet Controllers, United States	Rule #1 Suspicious Hosts Flow TO Source Host is using http (80/tcp) as client to nuq04s06-in-f10.1e100.net (Double-click for details)

案例:检测数据丢失



检测数据丢失

Alarm Type IP Address Username Flow Table Policy violation details

Host Group Dashboard Alarm Table

Filter Domain : Alpha First Active Time : Last 14 days
Source or Target Host Group : Inside Hosts

Alarm Table - 45 records

Policy	Start Active...	Alarm	Source	Source Host Gr...	Source User...	Target	Target...	Details
Inside Hosts	8-Feb-2012 5:05:00 PM (11 days 22 hours 48 minutes ago)	Suspect Data Loss	10.34.74.123	SJCM, Wired Data		Multiple Hosts		Observed 4.08G bytes. Policy maximum allows up to 81.92M bytes.
Inside Hosts	16-Feb-2012 11:40:00 AM (4 days 4 hours 13 minutes ago)	Suspect Data Loss				Multiple Hosts		Observed 16.8M bytes. Expected 4.86M bytes, tolerance of 50 allows up to 15.33M bytes.
Inside Hosts	8-Feb-2012 12:40:00 PM (12 days 3 hours 13 minutes ago)	Suspect Data Loss				Multiple Hosts		Observed 11.92M bytes. Expected 1.16M bytes, tolerance of 50 allows up to 10M bytes.
Inside Hosts	8-Feb-2012 12:10:00 PM (12 days 3 hours 43 minutes ago)	Suspect Data Loss						Observed 11.79M bytes. Expected 1.16M bytes, tolerance of 50 allows up to 10M bytes.
Inside Hosts	7-Feb-2012 8:50:00 PM (12 days 19 hours 3 minutes ago)	Suspect Data Loss						Observed 11.63M bytes. Expected 1.16M bytes, tolerance of 50 allows up to 10M bytes.
Inside Hosts	15-Feb-2012 3:10:00 PM (5 days 43 minutes ago)	Suspect Data Loss				Multiple Hosts		Observed 44.59M bytes. Expected 3.17M bytes, tolerance of 50 allows up to 12.14M bytes.
Inside Hosts	15-Feb-2012 2:35:00 PM (5 days 1 hour 18 minutes ago)	Suspect Data Loss				Multiple Hosts		Observed 26.91M bytes. Expected 3.17M bytes, tolerance of 50 allows up to 12.14M bytes.

Quick View This Row

- Disable Alarm(s)...
- Host Policy...
- Workflow
- Mitigation
- Notes
- Flows
- Associated External Events

for Host [redacted]:

- Host Snapshot
- Top Status
- Security
- Hosts
- Traffic
- Reports
- Flows
- Configuration
- External Lookup

Flow Table

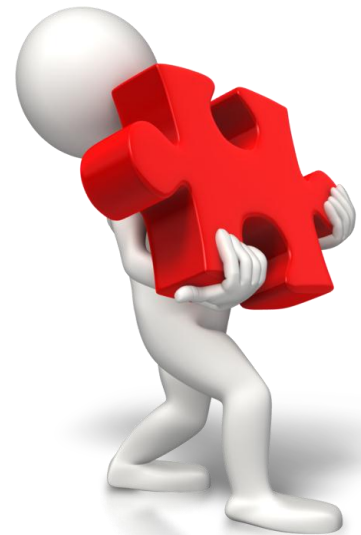
- Network and Server Performance
- Flow Traffic
- Peer Vs. Peer
- Peer Vs. Port
- Time Vs. Peer
- Time Vs. Port

Cyber Threat Defense 2.0: Scalable Network Defence

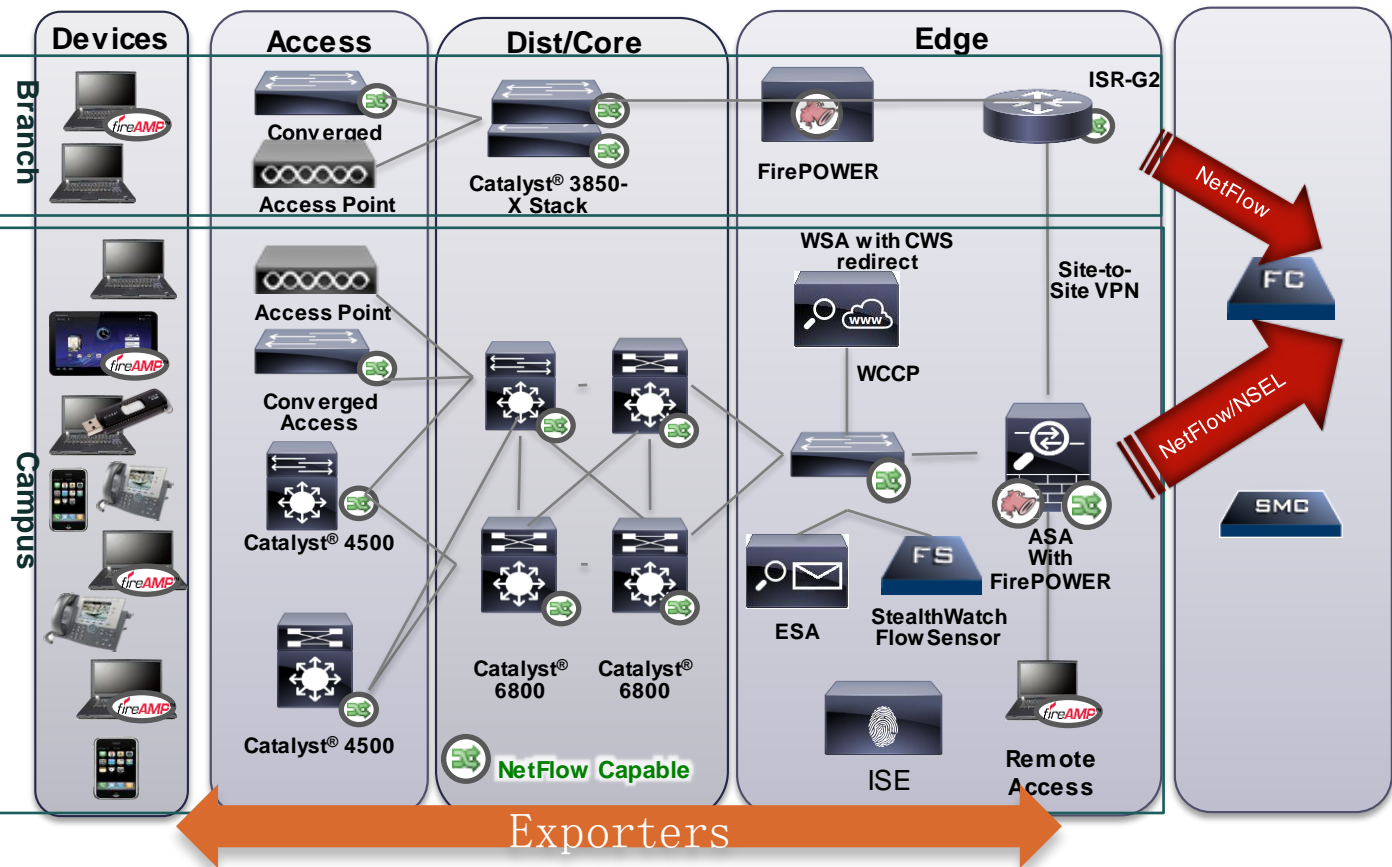


基于“数据流行为统计分析”（中医）
更多覆盖内部东西流量可视及威胁发现（面覆盖）

基于“特征库、漏洞库”（西医）
更多覆盖南北流量可视及可控、威胁发现（点覆盖）

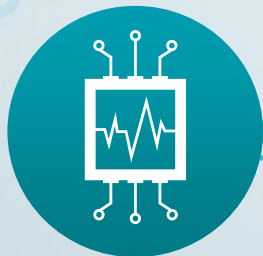


思科园区网解决安全



- ISE+802.1X实现网络安全接入
- 边界防火墙实现网络边界4-7层访问控制
- Sourcefire Firepower实现边界威胁防御（应用控制、入侵检测、恶意软件检测）
- CTD检查网络异常主机，东西流量异常检测，防止病毒产生流量冲击网络设备
- ESA实现邮件安全，防垃圾邮件、防病毒

Lancope StealthWatch应用场景



数据中心场景

公有 | 私有 | 混合

网络运维

- 网络流量统计
- 网络访问回溯
- 网络异常快速定位、取证

提供网络流量情景信息

检测网络中异常流量

检测网络中用户违规访问

网络安全

- 异常流量检测
- 蠕虫爆发
- 僵尸检测
- 数据窃取
- 非合规访问

有线 | 无线 | VPN

办公园区场景

总结

- **安全手到擒来 一键安全保护** 可以结合ISE 进行快速安全隔离 减缓威胁影响
- **集思广益 全民皆兵** 网络中的路由器 交换机 无线控制器 防火墙 只要支持flow协议的都可以作为安全的监测点
- **保护我们能看到的资产** 让网络通道也变的可视化

