Advanced Security Analytics: NetFlow and Metadata for Incident Response

Cybersecurity Summit : Boston

Agenda

- Shifting security strategies
- Mining data from your network infrastructure
- Flow and metadata export types and sources
- Data correlation, visualization and reporting
- Complement existing security platforms
- Least privilege reduce risks from IoT
- Data-driven approach to incident response

Failing Security Strategy

As an industry we have focused primarily on prevention

Out-of-control threat surfaces and sophistication of attacks

In today’s reality breaches are inevitable

plixer

Detection Alone is Not Enough

Detecting incidents is just the first step

Now what do I do, where do I start

Focus must shift to incident response

plixer

The Network Sees All

Every “1” and “0” you care about traverses the network

The network is your most reliable source of truth

Collect, summarize and export via NetFlow, IPFIX and metadata

plixer

Context is King

Latest buzzword bingo, but has real market traction

Single source of who, what, where, when, why and how

Effective incident response requires more context

plixer

NetFlow

v5

Invented by Cisco

L2-4 source/dest., TCP/UDP port & type, AS source/dest., packet count

Top talkers, bandwidth consumption, etc

NetFlow

v9

Cisco proprietary – not intended for other vendor exports

Template driven, exports fixed length elements

Supports sampled flows

plixer

IP Flow Information Export (IPFIX)

RFC 7011

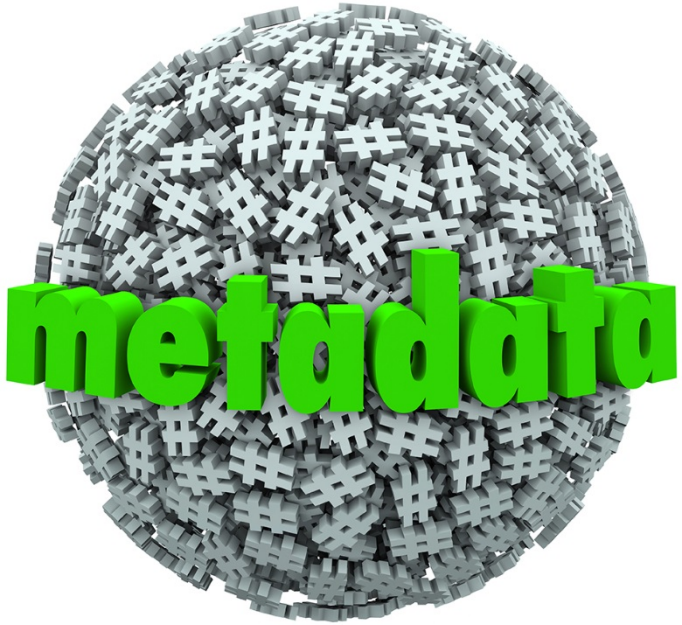
Industry standard established for exporting metadata

Template driven with support for user-defined fields

Exported data can be translated as a structured database

plixer

The Growth of Metadata



Vendors are striving for market differentiation

Proprietary data exports are rapidly growing

Context enables data driven incident response

Data Exporter Examples

Security Details in Flow and Metadata

Traffic Patterns (FTP beaconing)

Tor connections

DDoS detection

P2P lateral movement

URL details

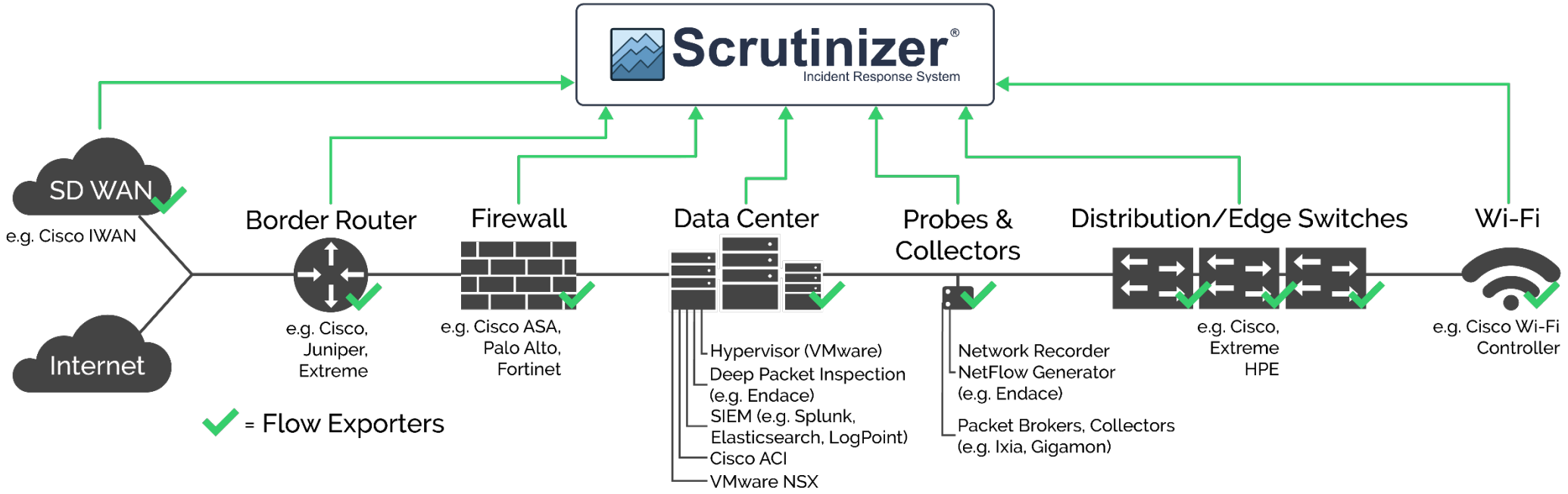
DNS queries

SSL details

Domain reputation

plixer

One Database



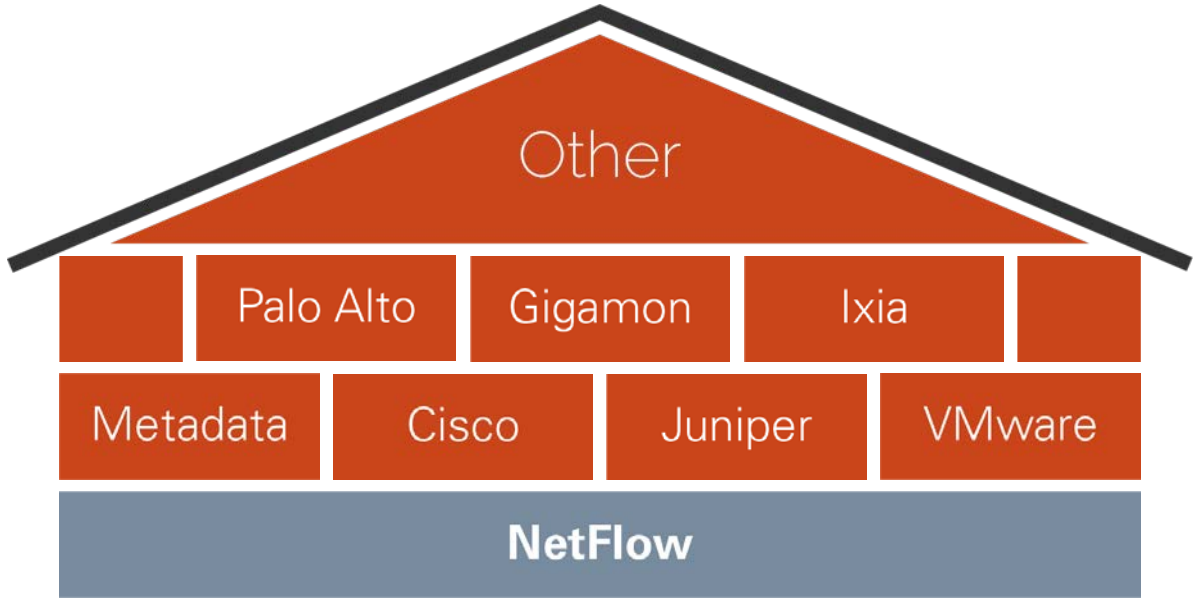
Data correlation

Visualization

Reporting

plixer

Incident Response - The House that NetFlow Built



NetFlow: the foundation providing source/dest to every conversation

Investigative forensics leveraging thousands of data elements

Context enables data driven incident response

Complement Existing Security

Rapid root cause analysis with timestamp

Pivot into SIEM and DPI for additional incident details

Take dynamic action to automate incident response (IPS, Firewall, etc.)

plixer

IoT Least Privilege Policy

Stop deploying IoT as trusted assets

IoT devices are purpose built with a narrow set of communications

Identify least privilege policy then monitor and alert for any deviation

plixer

Data Driven Incident Response

Desired goal is faster time-to-response

Contextual data is actionable data

Flow and metadata is emerging as a critical source of forensics

plixer

Collector/Reporting Engine Evaluation Criteria

How many elements are supported and from which vendors?

How well does reporting stitch together L2-7 metadata?

How quickly can you query the data and pivot on elements?

plixer

Bob Noel, Director Strategic Partnerships and Marketing
bob.noel@plixer.com
www.plixer.com

plixer