Cyber Security & Data Summit – June 18

Cyber Security at large scale

Agenda

Telesoft Introduction

Large scale

Challenges for Network Visibility in Large Scale Networks

How to Overcome Network Visibility Challenge

Open Source

Telesoft Solution

telesoft

Telesoft Technologies

Company Overview

We are a proven and trusted global provider of government infrastructure, cyber security and telecoms mobile products and services.

We work with integrators and Service Providers to develop, manufacture and support systems that generate revenue, keep critical infrastructure operational and important data safe on legacy high density TDM, optical SONET/SDH and latest technology multi 100Gbps networks.

Background

Established in 1989

Partnering with the world’s leading telecom operators, equipment vendors and Government Agencies (SIGNIT/Cyber Defence) for over 29 years

Ownership of IPR hardware & software

Re-invest approx. 20% of revenues in R&D

Staff (75% engineering)

Rich mixture of network and telecom experience

World-wide sales & support

Offices in UK, USA & Asia Pacific

Value proposition

- Self-sustained privately held Company
- 29 years of experience in High Technology
- Technology expertise in Government Infrastructure, Telecom & Cyber
- In-house developed stacks & hardware platforms
- FPGA based modular and adaptive design
- Proactive engineering team
- Global project management expertise
- Customer friendly open minded support team (24x7)
- Presence in Asia Pacific, UK and Americas

Large Scale?

Millions of events per second (network + security)

Disparate data sources and threat indicators

Heavily mixed traffic – business, VNOs, private, services

10’s M of subscribers

National ISP/CSP

Multiple Data Centres, 100,000’s of servers

Network Infrastructure & other CNI

The visibility challenge with high rate data

Enterprises use multiple tools in their Security Operations Centre (SOC) to protect their networks and data.

An analysts work flow includes traffic flow analysis, accessing and analysing event and log data, using a Security Information and Event Management system (SIEM).

Equipment commonly available to run these tasks does not scale well, or at all, to the volumes of data seen across a carriers network or a large scale datacentre.

The current option is to purchase multiple low throughput cyber defence tools and additional monitoring infrastructure to load share traffic across each element.

This is usually not economically viable.

Hence - as networks expand and security threats rise, CISOs and IT security professionals are losing visibility, knowledge and control

What Do CSPs & Cyber Defence Agencies tell Us They Want?

Want visibility across my entire network

Want real time analysis and threat indicators

Want to understand traffic patterns

Want Solution which provides Actionable Intelligence

Want access to historical data for Incident Response

Want answers in as short a time as possible – sub second

But full DPI and record at multi 100Gbps are prohibitively costly

One Answer… Flow Data

Flow meta-data reduces each IP communication session to summary

Of from, to, how much and when.

Industry standards

- IPFIX
- NetFlow – Cisco (top talkers, b/w…)

Can be expanded to include additional data for cyber ops: SSL certificate, DNS, http/https url…

Analyzing Flow Data Gives Us

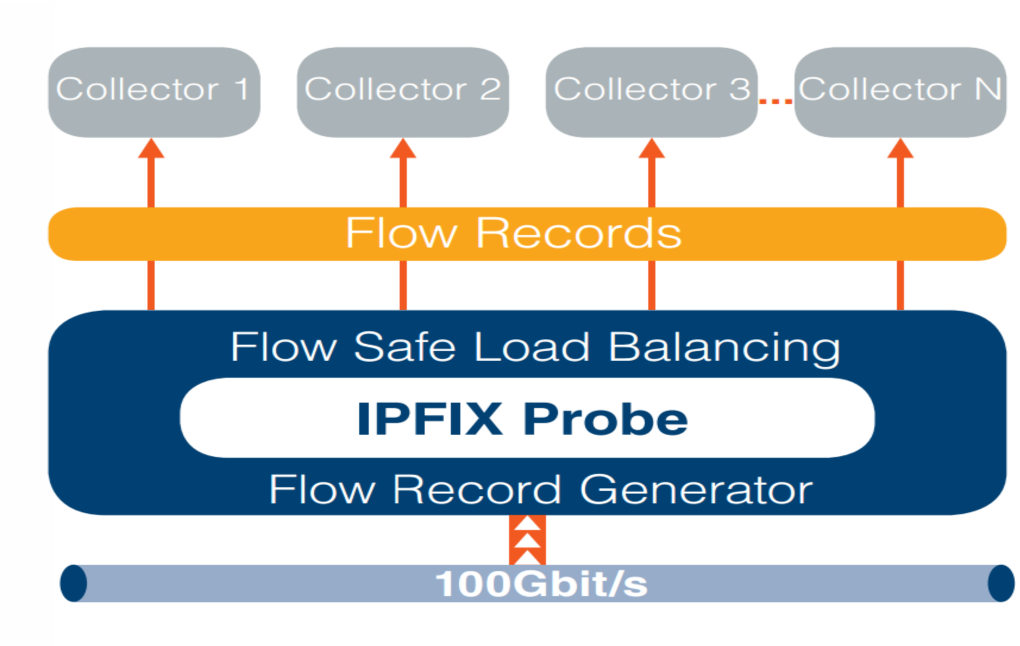
- Real time processing
- Anomaly detection
- Zero day threat
- DDoS detection
- Botnet detection
- DNS query
- SSL exchange
- Traffic Patterns
- Stored records
- Incident Response

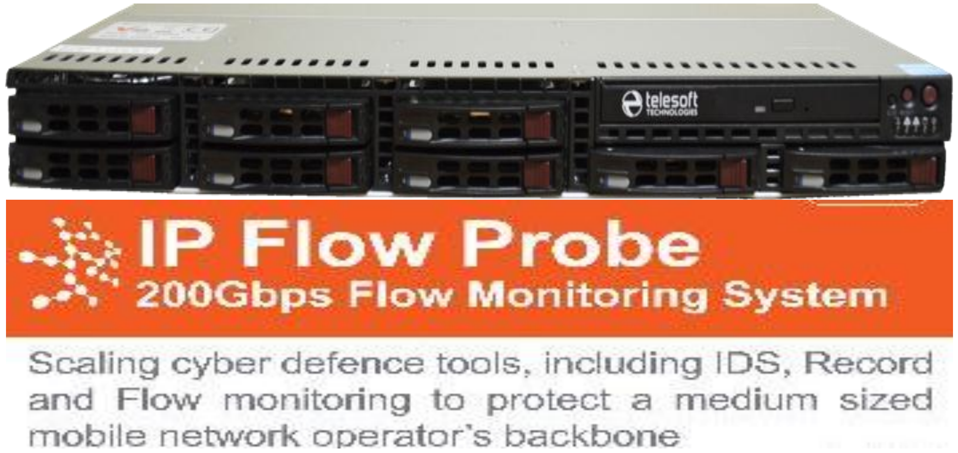
Telesoft Product Portfolio

Why we are different

- Systems are designed to dynamically scale in large throughput blocks
- No sampling - full visibility, analysis and investigation of network activity
- Meet government requirements for access control ,auditing, logging and retention
- 200G systems in 1U platform

Telesoft 1U Flow Probe

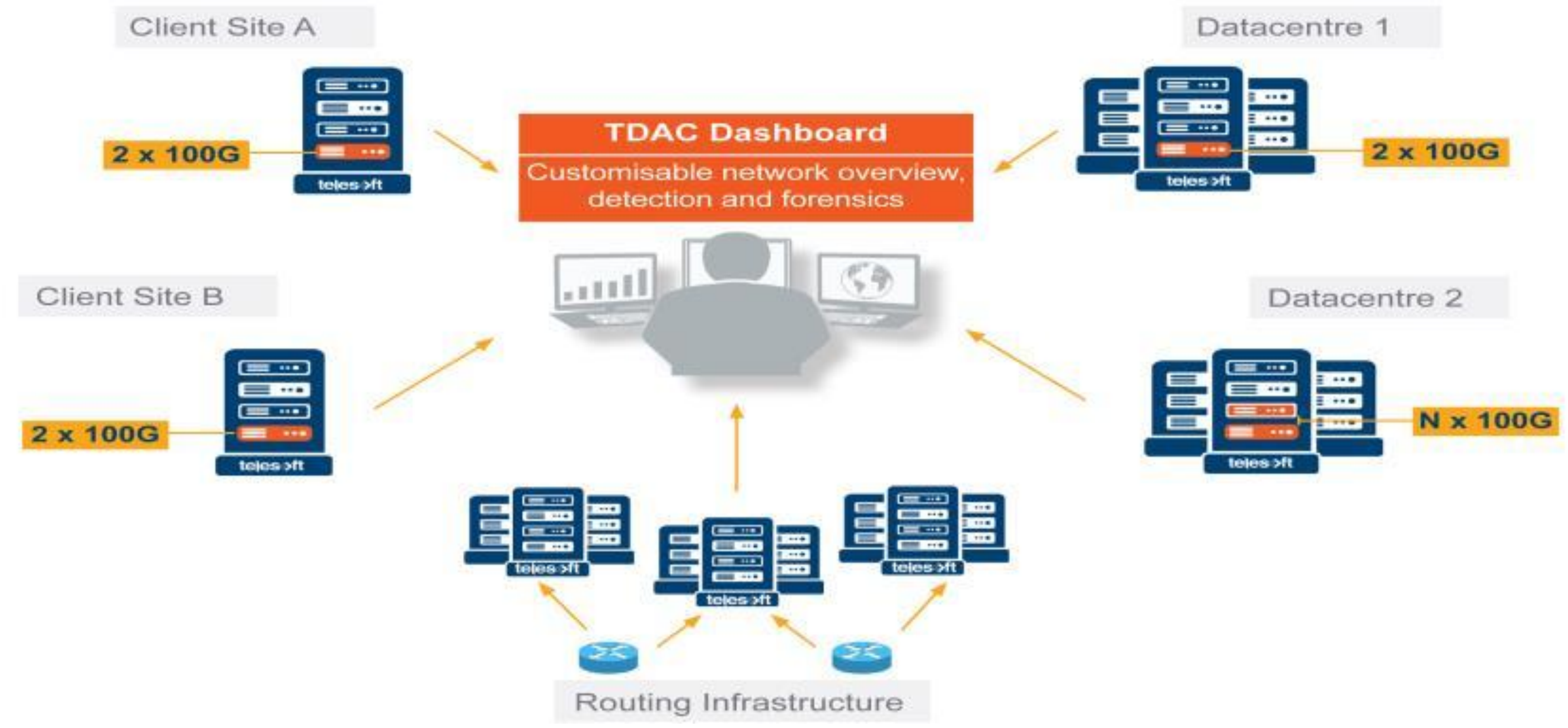




Scaling cyber defence tools, including IDS, Record and Flow monitoring to protect a medium sized mobile network operator's backbone

Multi 100Gbps Visibility/Cyber Security

TDAC Example Configuration



telesoft

Key Features & Performance

Single 1U appliance for 2 x 100GbE or 20 x 10GbE

Enables *ultra-scale* network cyber security

100% accurate. No missing or estimated records

Enables cost efficient storage of data for historical analysis

Independent of infrastructure as entirely passive = Low deployment risk

A single 1RU flow sensor appliance provides:

- 2 x 100GbE
- 2.5M flows/s sustained
- 3.5M flows/s peak
- 150M concurrent flows

Summary

Summary

- Large scale – M’s of events, 10M’s endpoints/users/subscribers
- Need to protect end users, brand, reputation, CNI at large scale
- CSPs ask for visibility across entire network
- Some tools struggle to scale up
- IP Flow monitoring can help – standards, multi-vendor
- May need dedicated flow exporters for accuracy
- Enrich data from other sources
- Analyse in real time and store for historical analysis

Thank You!

At Telesoft, we ensure that the organizations that carry the worlds largest volumes of data such as national CSPs and large datacenter operators have continuous visibility of the traffic on their network. And we combine that data with threat intel – to give indicators of compromise and rapid incident response.

Rohit Singh

Country Manager- Asia-Pac & India

Mob: +91- 9873173042

DDI: +91- 120-6127725

Fax: +91-120-61277023

Email: rsingh@telesoft-technologiers.com

www.telesoft-technologies.com