TELESOFT

CRITICAL NATIONAL INFRASTRUCTURE SELECTS TELESOFT

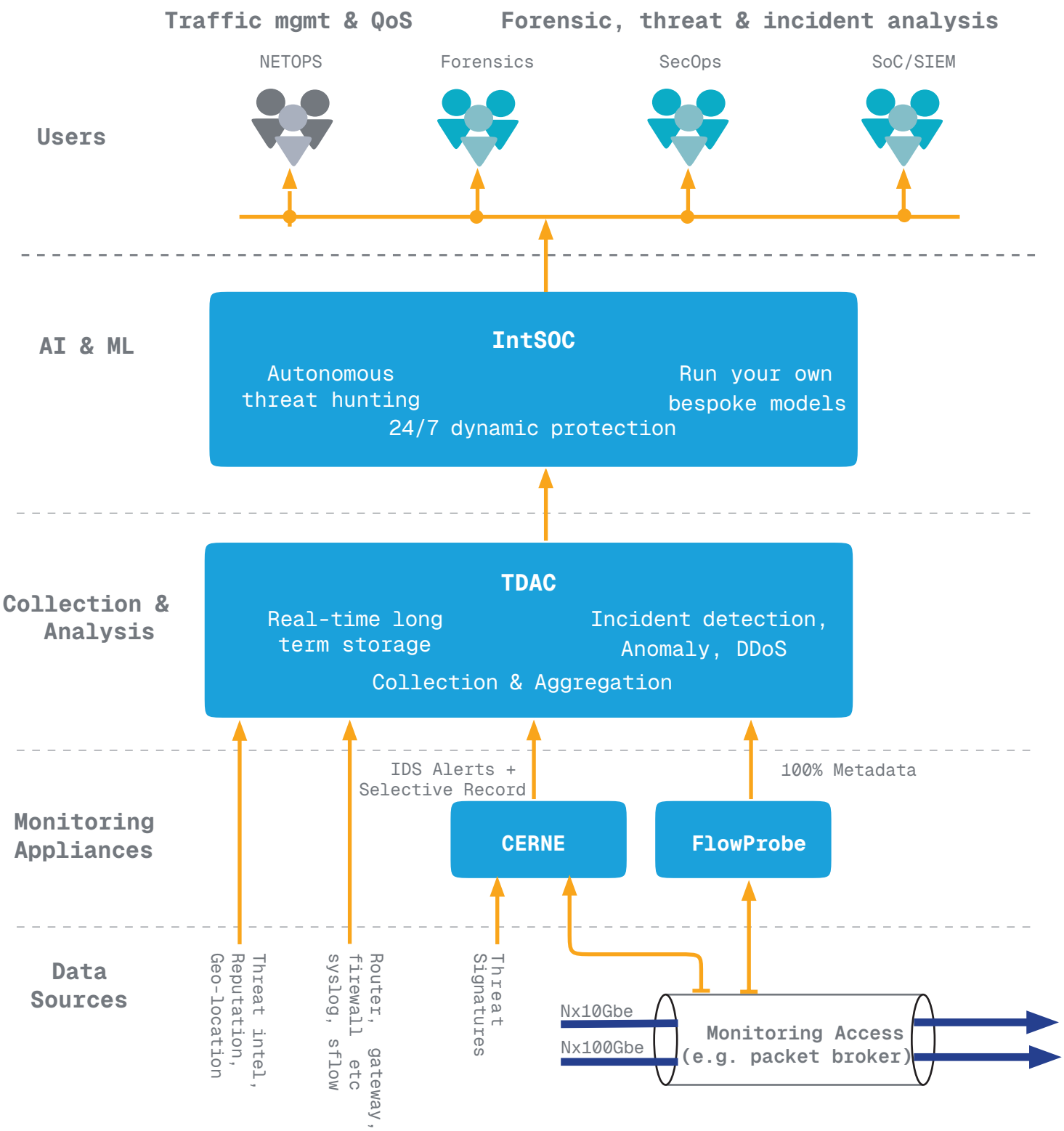
CYBER SECURITY SOLUTION BRIEF

TELESOFT

PROTECTING CNI

GLOBAL COMMUNICATIONS PROVIDER SELECTS TELESOFT

The solution includes FlowProbe for network flow analysis, CERNE for high-rate IDS and event capture, TDAC for multi-100Gbps monitoring and long-term storage, and IntSOC for AI-driven threat.



THE CHALLENGE

PROTECTING CRITICAL NATIONAL INFRASTRUCTURE AT GLOBAL SCALE REQUIRES SPECIALISED CAPABILITIES

Sovereign control, multi-100Gbps scalability, and deep traffic visibility.

The operator's existing infrastructure presented significant challenges. Monitoring relied on sampled data that missed critical threats, while scattered tools provided only partial visibility across the global network.

THE NETWORK

```
[100M+ entities]  [Multi-100Gbps]  [Global operations]

[Sampled data]    [Mixed traffic]   [Limited visibility]
```

REQUIREMENTS

- Protect infrastructure from known and zero-day attacks while prioritising monitoring of rapidly changing physical and virtual assets
- Understand bad traffic volumes (DDoS) for scrubbing, hunt for anomalous behavior, and discover and disable botnets across the infrastructure
- Store metadata for minimum 3 months with rapid historical query capability for post-incident analysis and incident response
- Integrate with existing legacy tools and support multiple teams across different sites

THE SOLUTION

Using Telesoft's FlowProbe, CERNE, TDAC and IntSOC the provider achieved comprehensive network visibility with full sovereign control and multi-100Gbps scalability.

THE SOLUTION

NETWORK VISIBILITY

Comprehensive monitoring across hundreds of millions of entities

Telesoft deployed FlowProbes at strategic national gateway points to capture unsampled metadata from every network session. This provides complete visibility while reducing data volumes 100:1 compared to full packet capture, enabling comprehensive monitoring without overwhelming storage infrastructure.

STORAGE AND ANALYSIS

High-speed query and intelligent data management

TDAC's distributed architecture stores 3 months of metadata with sub-second query response times. User-configurable entity grouping enables prioritised monitoring of high-risk assets and infrastructure, making it possible to track specific threats across millions of events per second.

THREAT DETECTION

Multi-layered approach to known and unknown threats

The solution combines multiple detection methods. Anomaly detection uses AI-driven pattern analysis to identify zero-day threats and unusual behaviour. CERNE IDS detects known threats at 200Gbps per appliance through signature matching. IP reputation provides automated alerts for traffic from known malicious sources, while selective capture enables event-driven packet recording of suspicious sessions only.

INTEGRATION

Multi-user access across global security teams

Custom dashboards, configurable alerts, and API integration enable security teams across global sites to collaborate effectively while maintaining role-based access controls and query prioritisation.

"They have a reputation for delivering - they do deliver"

VP Network Planning, Global CNI