

SharkFest'26 Europe

The Perimeter Is Dead. Long Live the Perimeters.

Christian Landström
Head of CERT
Siemens AG

Sponsored by:
PROFITAP DEEP NETWORK OBSERVABILITY
cPacket
TCP/IP training
endace Record. Respond.

Agenda

- **Introduction:** How the perimeter changed
- **Current state:** Current threat model
- **Challenges:** Visibility and control architecture
- **Things you can do:** Pragmatic implementation roadmap

Perimeter Security

Same challenge. Different edges.

From a wall to a distributed defense.
Deciding where visibility and control
create real security value.



People
Everywhere

Data
Everywhere

Attackers
Adaptt Faster

Security
Must Be Smarter

MORE VISIBILITY.
REALER IMPACT.
GREATER RESILIENCE.

The Perimeter Has Changed

It didn't disappear – it fragmented.

SIEMENS
Technology for a safer tomorrow

Then: The Castle Wall

A clear boundary, few entry points.



Now: Many Edges

Identity, cloud, devices, data, APIs, and more.



Traditional Perimeter		Distributed Perimeter
Clear physical and network boundary	›	Many distributed enforcement points
Few, well-defined entry points	›	Numerous and dynamic entry points
Mainly on-premises infrastructure	›	Hybrid and multi-cloud environments
Control focused on north–south traffic	›	Both north–south and east–west traffic
Easier to monitor and manage	›	Higher complexity and more telemetry
Known users, devices and locations	›	Diverse users, devices, locations and third parties

The perimeter did not disappear. It evolved.

The challenge is to decide where visibility and control create measurable security value.

“The perimeter is dead” is a lazy statement

The traditional perimeter is no longer sufficient. But organizations still have boundaries, trust transitions, enforcement points, and choke points.

The difference is that there is no longer **one** perimeter.

Today’s enterprise has multiple overlapping perimeters:

- Identity perimeter
- Device perimeter
- SaaS perimeter
- Cloud-control-plane perimeter
- Workload and container perimeter
- Application and API perimeter
- Data perimeter
- Browser perimeter
- Third-party and supply-chain perimeter
- OT and legacy perimeter

A practical implementation sequence - Do the boring things first

Phase 1 – Establish facts

- Identify business-critical resources
- Identify internet-facing assets
- Identify privileged and non-human identities
- Map critical data flows, cloud accounts, subscriptions, tenants, and trust relationships
- Document existing observation and enforcement points

Phase 2 – Close fundamental gaps

- Improve asset ownership and inventory
- Enforce strong authentication
- Increase endpoint and workload coverage
- Reduce excessive privileges
- Patch exploitable internet-facing systems
- Remove unnecessary exposure
- Enable essential cloud-control-plane logging

Phase 3 – Instrument prioritized attack paths

- Select telemetry based on detection use cases
- Define ownership and escalation
- Build investigation and containment workflows
- Test detections through realistic exercises
- Measure coverage, latency, and analyst effort

Phase 4 – Optimize

- Remove duplicate telemetry
- Tune retention by evidentiary value
- Consolidate overlapping tools
- Automate repeatable response actions
- Reassess controls when architecture and threats change

A realistic threat model - What are we actually defending against?

Initial access

- Phishing and adversary-in-the-middle attacks
- Credential theft and session-token theft
- Exploitation of internet-facing applications
- Exposed cloud services
- Compromised third parties
- Malicious or vulnerable dependencies
- Unmanaged endpoints and shadow IT

Post-compromise activity

- Privilege escalation
- Cloud-role abuse
- Persistence through identities and automation
- East-west movement
- SaaS-to-SaaS movement
- Data discovery and staging
- Command-and-control traffic
- Exfiltration through approved services
- Destructive or disruptive actions

Do not buy “AI security” to compensate for missing fundamentals.



GenAI may compress attacker timelines. It does not invalidate the basic attack lifecycle.

Emerging acceleration factors

- Faster reconnaissance
- Faster vulnerability research
- Automated attack-path discovery
- Scalable social engineering
- Rapid creation and modification of malicious tooling
- Abuse of AI agents, model connectors, plugins, and machine identities

The visibility problem



You cannot monitor everything equally

Telemetry sources competing for budget and attention:

- Firewall and proxy logs
- DNS telemetry
- NetFlow and cloud flow logs
- Full packet capture
- Endpoint network telemetry
- Identity and authentication logs
- Cloud-control-plane logs
- SaaS audit logs
- […]

Challenge: More telemetry does not automatically produce more detection.

It can also produce:

- Higher ingestion and retention costs
- Duplicated signals
- Unclear ownership
- Alert flooding
- Longer investigations
- Collection without response capability
- Dependence on vendor-specific analytics

Detection-Driven Visibility

Start with the questions, not the tools.

SIEMENS
Technology for a safer tomorrow

FROM VISIBILITY
TO MEASURABLE
SECURITY OUTCOMES.

1 Understand the risks

What are we protecting?
What are the likely attack paths?

- Crown jewels and critical processes
- Threat actors and motivations
- Likely attack paths and scenarios
- Business and regulatory impact

2 Define detection objectives

What do we need to detect early?
What would we most regret missing?

- Priority use cases (e.g. initial access, lateral movement, data exfiltration)
- Detection goals and success criteria
- Time to detect and respond (TTD/TTR)
- Relevant stakeholders (SOC, CERT, business)

3 Identify required telemetry

Which data sources give us the visibility we need?
Where are the gaps?

- Map use cases to required data sources
- Assess current coverage
- Identify blind spots and constraints
- Prioritize high-value telemetry

4 Implement and test

Collect, tune, validate and improve.
Measure value and reduce noise.

- Ingest and normalize data
- Tune detections and reduce false positives
- Validate with real-world testing (e.g. purple teaming)
- Measure and demonstrate security value



RIGHT
VISIBILITY
RIGHT DECISIONS
A SAFER TOMORROW.

Visibility is valuable when it helps you detect and respond to real threats.
Focus on outcomes, not on collecting data for its own sake.

Start with detection questions, not log sources

The correct order of decisions

- What attack or failure are we trying to detect?
- What observable behavior would it create?
- Which telemetry source can reliably expose that behavior?
- How quickly must it be detected?
- Who investigates the signal?
- What response can actually be performed?
- What does collection, processing, and retention cost?
- Does another control already provide equivalent evidence?

Example

Threat: Compromised cloud workload contacting attacker infrastructure

Possible evidence:

- EDR network event
- Cloud flow record
- DNS query
- Secure web gateway event
- Cloud workload-protection alert
- Application log
- Packet capture

High-Value Observation Points

Focus where it makes a difference.

SIEMENS
Technology for a safer tomorrow

BETTER
VISIBILITY.
LOWER RISK.
HIGHER IMPACT.

PRIORITIZE THESE AREAS

Identity
Logins, privileged access, identity anomalies

Edge and network
Unusual connections, C2, lateral movement

Cloud
Misconfigurations, unusual API activity, data access

Endpoints
Execution, persistence, credential access

Applications and APIs
Abuse, injection, unusual behavior

Data
Sensitive data access, exfiltration attempts



FOCUS HERE.
Maximum security value.

Identity
Stop account takeovers

Edge and network
Detect movement early

Cloud
Find misconfigurations and risky activity

Endpoints
Catch execution and persistence

Applications and APIs
See abuse and exploitation

Data
Protect what matters most

COMMON BUT LOWER VALUE

Email content
High volume, lower signal

Routine system logs
Often too noisy

Generic internet traffic
Important, but rarely decisive on its own

Standard user activity
Mostly business as usual

Infrastructure health logs
Valuable, but not a primary threat indicator

TURN
VISIBILITY
INTO
RESILIENCE.

Not everything everywhere – but the right things in the right places.
Prioritize visibility where it reduces risk, not where it just looks good on a dashboard.

Traditional Network-Visibility Blind Spots

What you often don't see – but should.

SIEMENS
Technology for a safer tomorrow

SAME THREATS. DIFFERENT PLACES.



You see this ...
Known traffic.
Known users.
Known systems.

... but much happens here.
Modern work, cloud, SaaS and third parties extend the attack surface beyond traditional visibility.

Traditional Perimeter

Remote users and devices

Cloud platforms (IaaS / PaaS)

SaaS applications (often outside visibility)

Third parties and suppliers

Internet and unknown

Visible
What you typically see and monitor.

Hidden
What often remains unseen – but can have the biggest impact.

Encrypted traffic
Malicious activity hidden in TLS/HTTPS

Shadow IT
Unsanctioned applications and services

Remote users and devices
Outside corporate network, less visibility

Third-party and supply chain
Access via trusted partners

Cloud-native activity
Misconfigurations, unknown assets, data exfiltration

SaaS usage
Data in external applications (e.g. M365, Salesforce, etc.)

API traffic
Abuse, credential stuffing, automated attacks

Unknown actors
New entry points, new attack techniques (e.g. GenAI)

The biggest risks are often the ones you cannot see with traditional perimeter monitoring.
Expand visibility, correlate across environments, and focus on what matters.

BROADER VISIBILITY. STRONGER SECURITY.

A pragmatic visibility architecture in four complementary layers

Layer 1 – Identity and access - Minimum capabilities:

- Strong authentication
- Conditional access
- Privileged-access controls
- Service-account and workload-identity inventory
- Token and session visibility
- Authentication-event retention

Layer 2 – Endpoint and workload - Minimum capabilities:

- EDR on supported systems
- Runtime visibility for containers and cloud workloads
- Process-to-network correlation
- Remote containment
- Evidence collection

Layer 3 – Network and cloud - Minimum capabilities:

- Ingress and egress visibility
- DNS visibility
- Cloud-control-plane logs
- High-risk flow visibility
- Segmentation enforcement
- Selected packet capture for critical environments

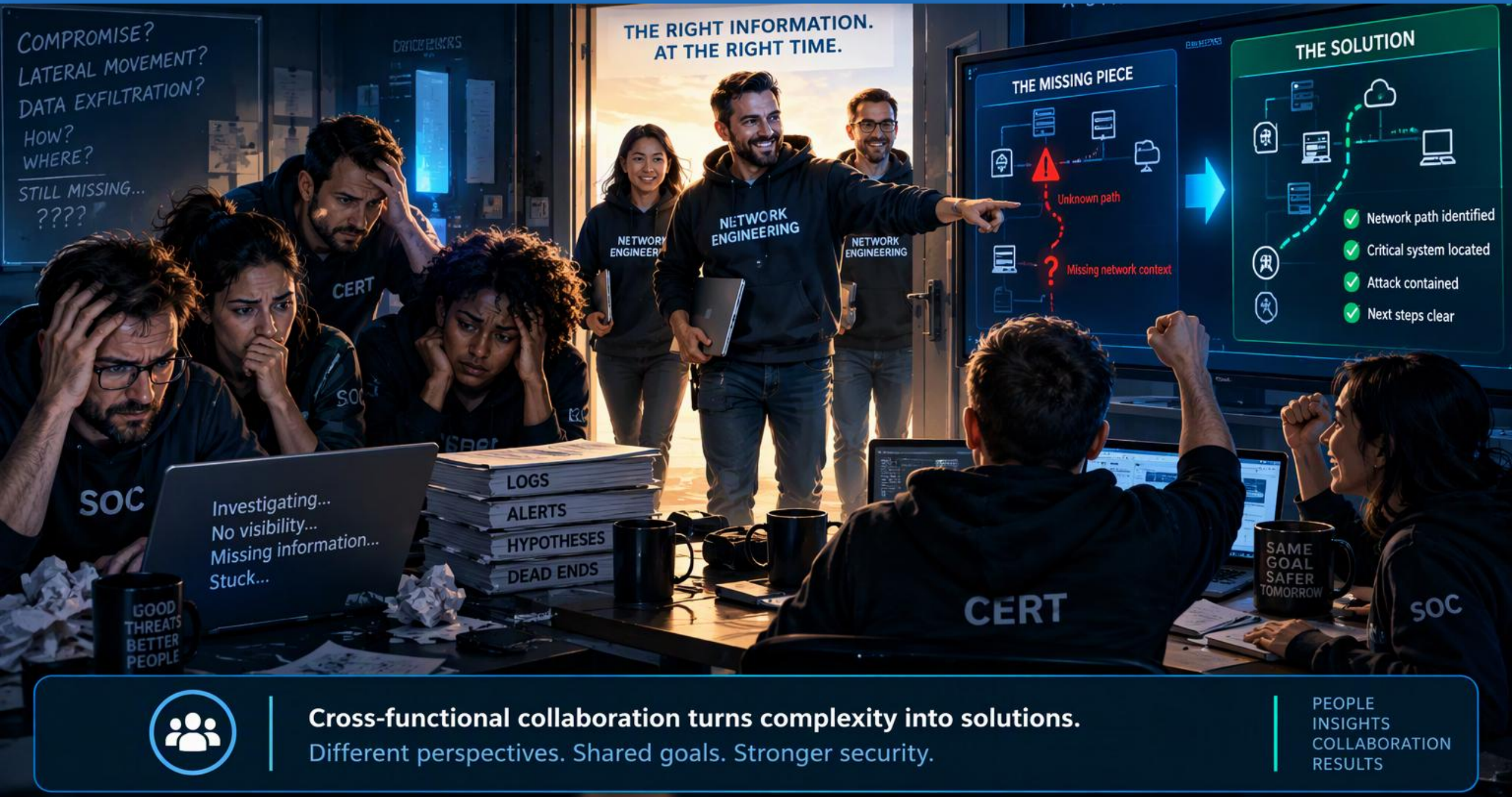
Layer 4 – Application, API, data - Minimum capabilities:

- Application authentication events
- API gateway telemetry
- SaaS audit records
- Data-access logging
- Sensitive-data movement controls
- AI interaction governance where justified

Five decisions for Monday morning

- Identify the five attack paths with the highest enterprise impact.
- Map the required signals and controls for each attack path.
- Find telemetry that is collected but not operationally used.
- Find critical systems without identity, endpoint, cloud, or network visibility.
- Stop throwing yet another technical solution to legacy, organizational/people/process problems.

Any questions before we ramp up?


COMPROMISE?
LATERAL MOVEMENT?
DATA EXFILTRATION?
HOW?
WHERE?
STILL MISSING...
????
THE RIGHT INFORMATION.
AT THE RIGHT TIME.
THE MISSING PIECE
Unknown path
Missing network context
THE SOLUTION
Network path identified
Critical system located
Attack contained
Next steps clear
NETWORK ENGINEERING
CERT
SOC
Investigating...
No visibility...
Missing information...
Stuck...
LOGS
ALERTS
HYPOTHESES
DEAD ENDS
GOOD THREATS BETTER PEOPLE
SAME GOAL SAFER TOMORROW
Cross-functional collaboration turns complexity into solutions.
Different perspectives. Shared goals. Stronger security.
PEOPLE
INSIGHTS
COLLABORATION
RESULTS

Thank You!

WIRESHARK

