



NetEye Conference 2026

AI & Human Insight: la coesistenza strategica per le IT Operations

PIR:

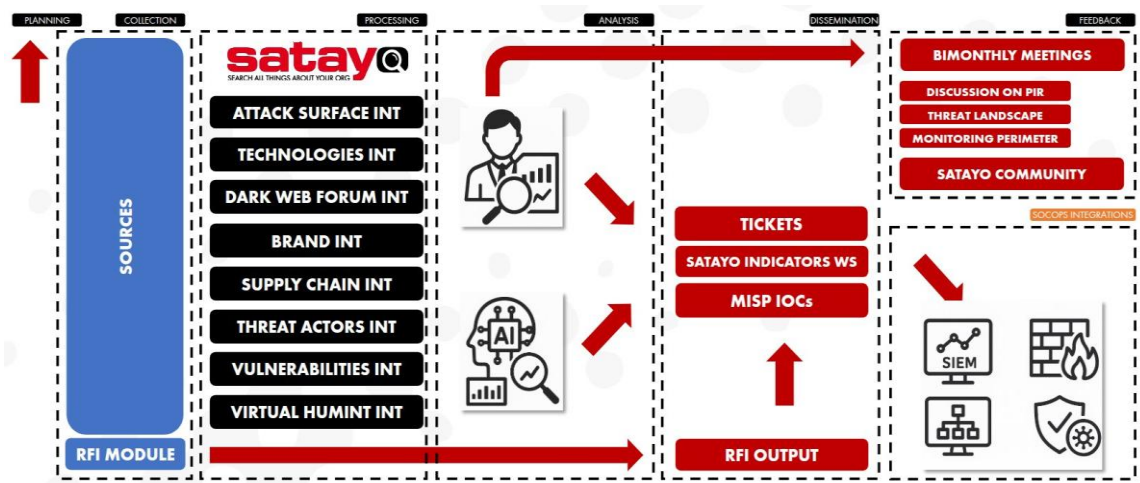
A Practical Guide to Building Intelligence-Driven Security Operations

Massimo Giaimo



The promise of this session

That's how we left things last year...



By the end of this talk, I would like you to have a clear idea of:

- What a PIR is
- How a PIR is defined
- How to implement PIRs within a **12-week roadmap**

PRIORITY INTELLIGENCE REQUIREMENTS

A Practical Guide to Building Intelligence-Driven Security Operations

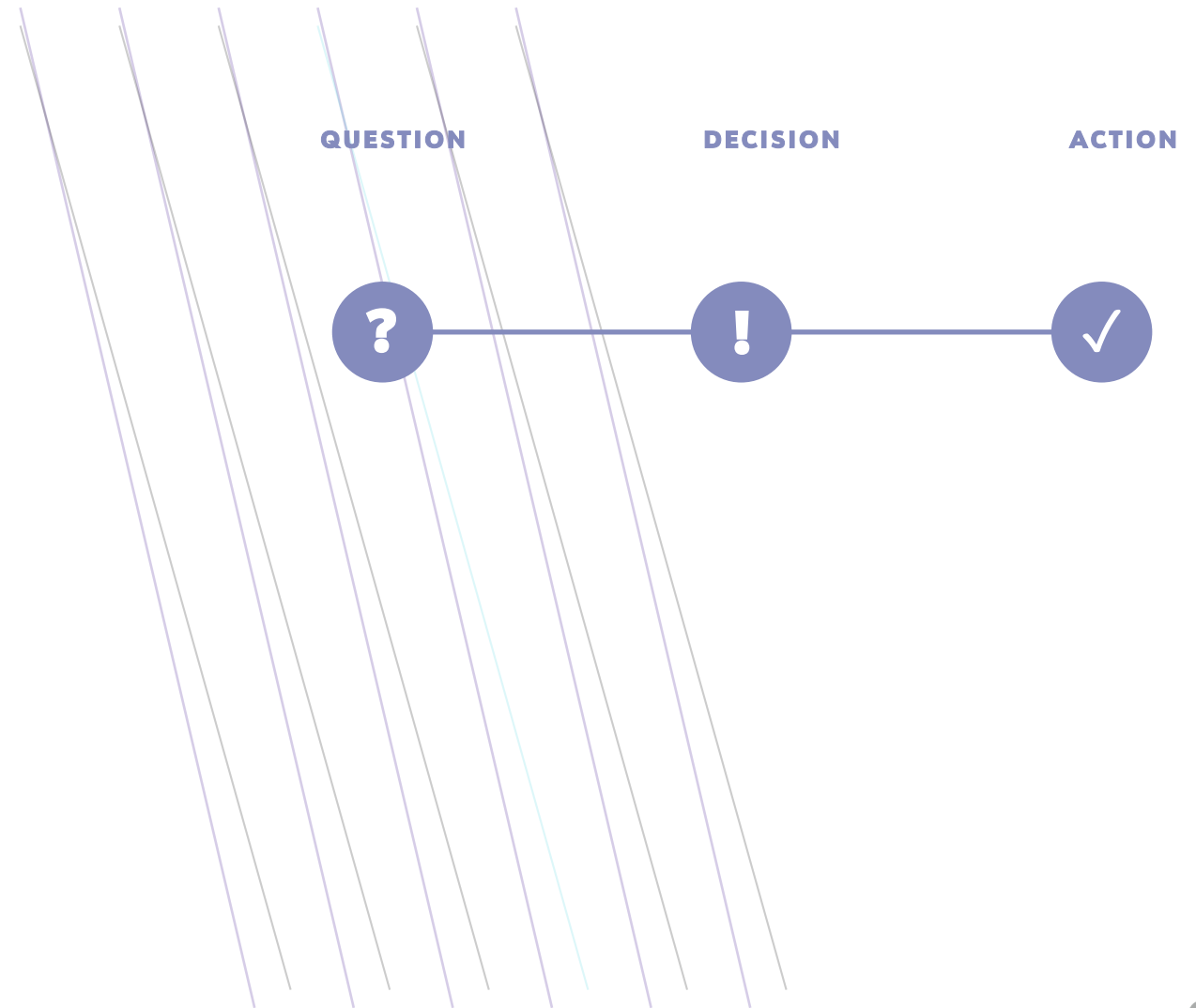
Massimo Giaimo

Head of Cyber Threat Intelligence, Würth IT

What is a PIR?

Before discussing PIRs in depth, it is important to clearly understand the difference between **data, information, and intelligence**.

A **Priority Intelligence Requirement** is the most important information need to support a **decision, achieve an objective, or asses a risk**.



Meet Northbridge Group



The fictional organization we will take from intent to operation

OPERATING PROFILE

An international industrial and logistics group
Headquarters in Europe 14-country (16 locations) footprint
Production and warehouse facilities in Europe and the Middle East
Shipping
Partners connected to the Strait of Hormuz
Suppliers across Eastern Europe, Asia and the Middle East



CRITICAL DEPENDENCIES

Remote access and VPN systems
Production and warehouse technology
Supplier and customer portals
Vessel tracking and cargo management
Cloud services Public websites, brands and executive identities

THE PRESSURE

Many information sources
Multiple stakeholders
Different subsidiary priorities
Shared infrastructure and suppliers
A changing geopolitical environment
Limited analyst attention

The Starting Point: More data than decisions

Prioritization is the bottleneck

TODAY

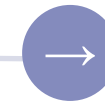
Inconsistent questions

- Threat feeds and reports arrive continuously
- Stakeholders ask for different kinds of warning
- Subsidiaries define urgency differently
- No shared threshold tells the team when to escalate

THE GAP



What should we know?



Who decides?



What changes?

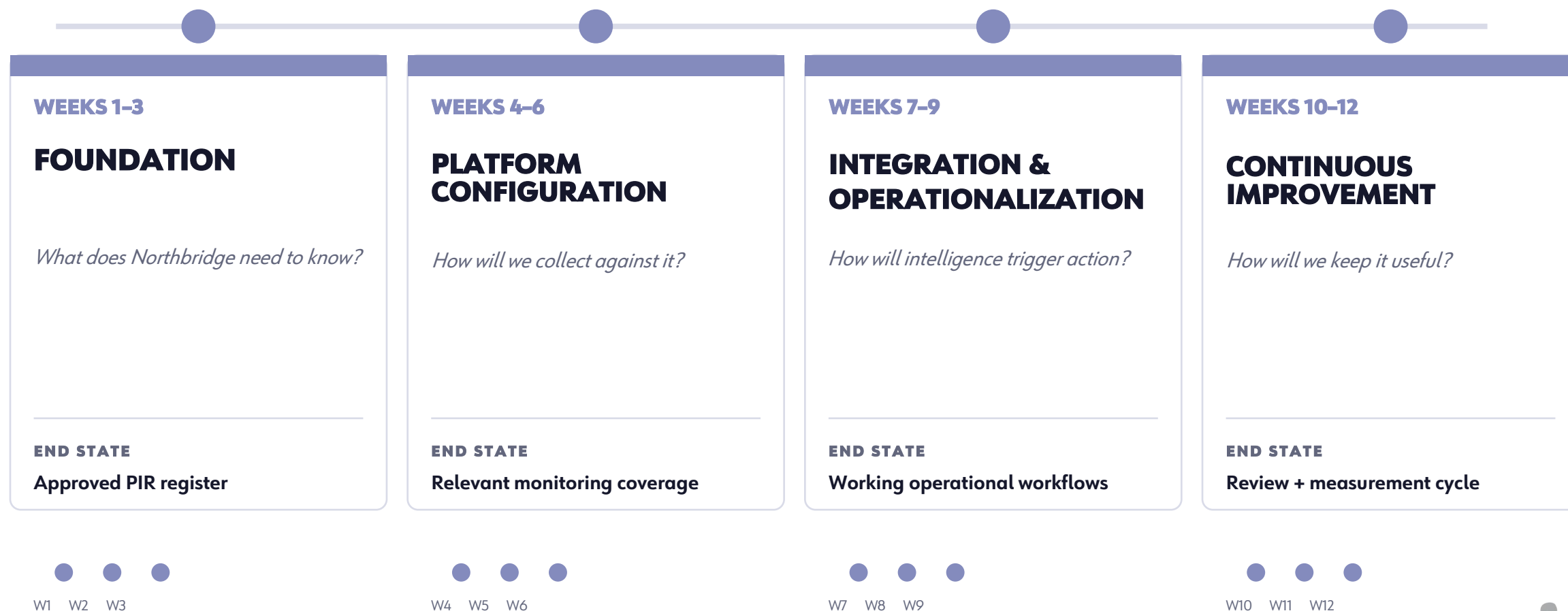
THE 12-WEEK ROADMAP

turns scattered information needs
into a governed operating capability



The 12-week journey from intention to operation

Four phases. Four end states. One operating PIR program.



Phase 1 - Foundation comes before collection

Create the governance, context, and approved priorities that make the rest of the program possible

PURPOSE

**Align the organization.
Before
configuring
the platform.**

No intelligence collection or broad platform configuration should begin until the foundation is in place.

OUTPUT

01

Sponsor + governance

02

Stakeholder requirements

03

Asset + technology context

04

Prioritized PIR register

Success looks like: approved PIRs, named owners, review dates



Weeks 1-3: build the decision foundation

Each week produces an artifact that makes the next week possible

WEEK 1

Governance

- Senior sponsor
- PIR program owner
- Approval + review rules
- Group / subsidiary roles
- Stakeholder schedule

DELIVERABLE

Governance document

WEEK 2

Requirements

- Stakeholder interviews
- Asset inventory
- Technology inventory
- VIPs, domains, keywords
- 10+ candidate PIRs

DELIVERABLE

Candidate PIR set

WEEK 3

Prioritization

- Score candidates
- Select initial set
- Write PIR statements
- Assign owner + date
- Stakeholder sign-off

DELIVERABLE

Approved PIR register



Phase 2 - Configure the PIR program

Translate approved intelligence needs into relevant, testable monitoring coverage

PURPOSE

Make the questions collectable.

Use Northbridge's asset, technology, identity, and brand context to make monitoring relevant.



THE CONFIGURATION LOGIC

Approved PIR



What must we answer?

Organizational context



What belongs to Northbridge?

Collection inputs



Where can evidence come from?

Initial output review



Does it answer the PIR?

Success looks like: documented coverage, gaps and relevant first outputs

Weeks 4-6: make the PIRs collectable

Northbridge adds context first, then tests whether the outputs are useful

WEEK	FOCUS	WHAT NORTHBRIDGE DOES	SUCCESS CHECK
WEEK 4	Core monitoring	Technology mapping VIP users Primary domains + IP ranges	Critical assets are covered
WEEK 5	Contextual monitoring	Keywords + name variants Ransomware Brand / favicon Mobile apps where relevant	Context is complete
WEEK 6	Finalize + test	Git repositories Configuration review Initial output review Coverage documentation	Outputs answer approved PIRs

Configuration is complete only when the first outputs are reviewed against the PIRs.

Phase 3 - Intelligence only matters when someone can use it

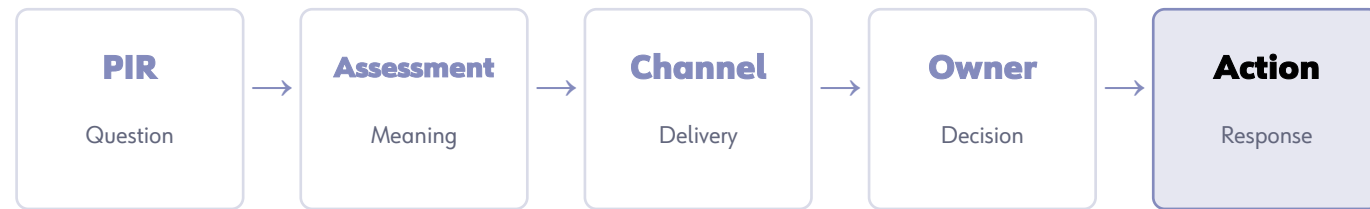
Connect every PIR to an owner, a delivery channel, a deadline and an action

PURPOSE

**Move from
output to
action.**

The operating model defines who receives what, how quickly and what happens next.

THE OPERATIONAL CHAIN



**A report is not a result.
A decision or action is the result.**



Weeks 7-9: connect intelligence to work

Northbridge tests the full path from PIR to action

WEEK 7

Dissemination

- Dissemination matrix
- Ticketing workflow
- Indicator sharing where required
- Escalation across subsidiaries

SUCCESS CHECK

Every PIR has a channel

WEEK 8

Launch + train

- RFI process
- SOC + IT training
- Consumer guidance
- Feedback mechanism

SUCCESS CHECK

Consumers can request + use intelligence

WEEK 9

Operational review

- Review each PIR
- Check output relevance
- Collect feedback
- Plan adjustments

SUCCESS CHECK

At least one improvement is identified



Phase 4 - The first 12 weeks end with a review, not a finish line

Turn implementation into a management cycle that stays aligned with Northbridge

PURPOSE

Keep the program useful.

PIRs should evolve when the organization, its decisions, or its threat landscape changes.

THE REVIEW LOOP

- 1 **Review** What happened?
- 2 **Measure** Was it useful?
- 3 **Adjust** What changes?
- 4 **Schedule** When do we look again?

A PIR is working when it improves a decision.



Weeks 10-12: prove the program is useful

The review must result in decisions, not only discussion

WEEK	FOCUS	NORTHBRIDGE DOES	OUTPUT
WEEK 10	Implement adjustments	Refine PIR wording Update configuration Close coverage gaps Record adjustment log	Updated PIR register + configuration
WEEK 11	Establish measurement	Define metrics per PIR Baseline the measures Create reporting template Separate group / subsidiary views	Measurement framework + baselines
WEEK 12	Formal review	Present data Review threat landscape Confirm relevance Schedule next cycle	Review report + next review date

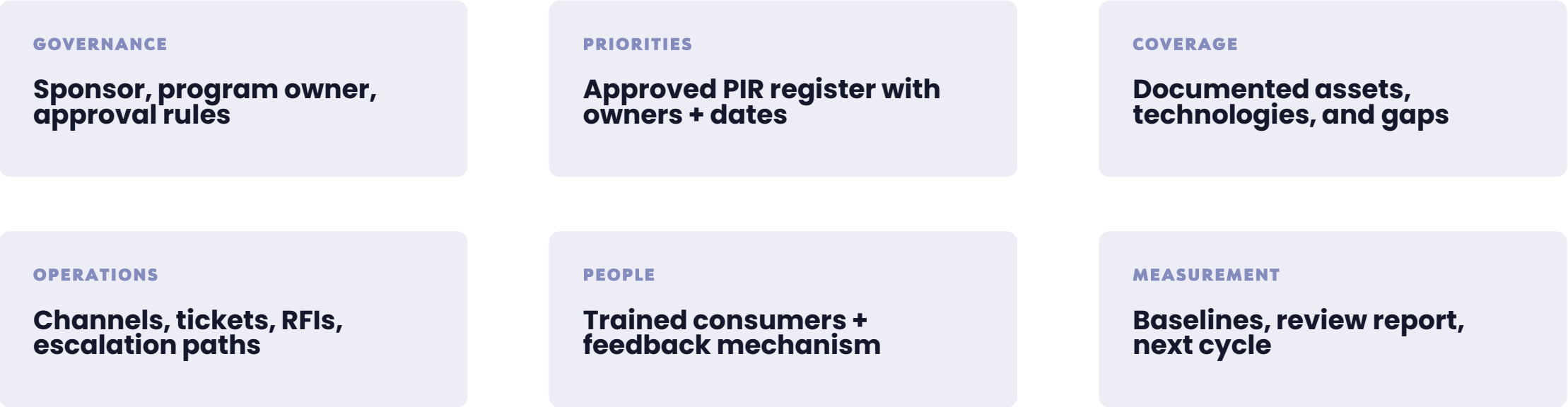
Measure decisions, not data volume.

Useful? Timely? Did it change what someone did?



What Northbridge has at the end of Week 12

The organization has built a capability, not just a configuration



Enduring PIRs + dynamic PIRs

A stable core with a controlled response to geopolitical change

ENDURING PIRs

Long-term questions about ransomware, critical suppliers, exposed technologies, and business disruption.

Reviewed on a normal cadence and changed when the underlying threat model changes.

DYNAMIC PIRs

Time-bound questions created when geopolitical conditions change.

Russia-Ukraine: state-aligned activity, sanctions, supply chain

Strait of Hormuz: maritime, port, energy, logistics

Palestine-Israel: hacktivism, influence, social engineering

TRIGGER PROCESS

Geopolitical trigger

↓

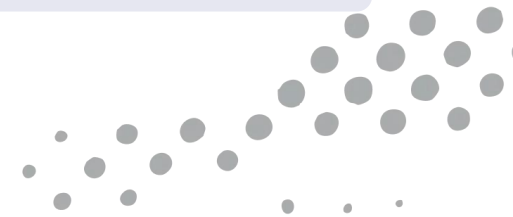
Rapid review within 48-72 hours

↓

Add · elevate · modify · reduce · retire

↓

Record owner + rationale + next review date



Do you need inspiration?

You can download a list of sample PIRs defined for Northbridge Group at the following link: <https://pirpracticalguide.satayo.cloud/docs/>.
I have also made available all the templates included in the book.

Name	Last modified	Size
 Parent Directory		-
 01_PIR_Statement.docx	2026-10-09 13:36	11K
 02_PIR_Prioritization_Checklist.docx	2026-10-09 13:36	10K
 03_Stakeholder_Interview_Record.docx	2026-10-09 13:36	10K
 04_Organizational_Asset_Inventory.docx	2026-10-09 13:36	10K
 05_Technology_Mapping_Worksheet.docx	2026-10-09 13:36	10K
 06_PIR_Register.docx	2026-10-09 13:37	9.9K
 07_Intelligence_Dissemination_Matrix.docx	2026-10-09 13:37	9.9K
 08_PIR_Review_Meeting_Agenda.docx	2026-10-09 13:37	10K
 Northbridge_Group_pirs.xlsx	2026-10-19 10:19	9.1K
 Northbridge_Group_profile.docx	2026-10-09 13:58	2.6M



A Practical Example: one PIR, four phases

How Northbridge turns a vulnerability question into an operating workflow

PIR IN SCOPE

Which newly disclosed or actively exploited vulnerabilities affect Northbridge remote access, VPN systems, production technology, warehouse technology, cloud services, portals or public-facing systems?

FROM QUESTION TO CONTROL

01

WEEKS 1-3 / FOUNDATION

Frame the question

NORTHBRIDGE DOES

- Name CISO, SOC and plant IT consumers
- Map VPN, OT, cloud and public assets
- Set owner, priority and review date

OUTPUT

Approved PIR + scope register

02

WEEKS 4-6 / CONFIGURE

Make it collectable

NORTHBRIDGE DOES

- Match assets to technologies
- Add CVE, exploit and advisory sources
- Test the first outputs against the PIR

OUTPUT

Coverage map + first alerts

03

WEEKS 7-9 / OPERATE

Make it actionable

NORTHBRIDGE DOES

- Route findings to the owner
- Add evidence, confidence and time
- Triggers the lifecycle of indicators (MISP, Threat Hunting rules)
- Escalate exploitation or impact

OUTPUT

Ticket + remediation clock

04

WEEKS 10-12 / IMPROVE

Keep it useful

NORTHBRIDGE DOES

- Measure timeliness and action
- Review gaps, noise and misses
- Update scope as risk changes

OUTPUT

Revised PIR + next review cycle

THE RESULT

A vulnerability signal becomes a named decision, action and review.

The Threat Intelligence Life Cycle applied to the book

When you have completed reading the book, you will have the opportunity to get your PIR Practical Guide Passport

PIR Practical Guide Passport



PHASES

- P** **What is your learning objective reading this book?**
- C** **Read the entire book with a practical mindset**
- P** **Complete the proposed exercises**
- A** **Create a real PIR for you organization**
- D** **Share an insight publicly (use #PIRPracticalGuide tag)**
- F** **Interact with the author**

SATAYO Community Connect #01

For the first time, the SATAYO Community meets in person. An afternoon of real-world security insights, live demonstrations and open exchange.
More info here: <https://www.wuerth-it.it/en/satayo-community-connect/>

SATAYO Community Connect

Ready to share. Ready to defend. Ready to collaborate.

For the first time, the SATAYO Community meets in person. An afternoon of real-world security insights, live demonstrations and open exchange.

Date

4 November 2026

Time

14:00 – 18:00

Location

Würth Italia, Egna (BZ)

Register now

Places are limited. Community members can bring a colleague.



14:00	14:15	Welcome coffee & registration
14:15	14:30	Opening & community update
14:30	14:50	The current state of the threat landscape
14:50	15:15	How does an attacker think?
15:15	15:40	From alert to response: what happens behind the scenes
15:40	16:00	Break
16:00	16:25	Integrating a private sandbox into artifact validation processes
16:25	16:45	SentinelWP – WordPress Security Sentinel
16:45	17:10	SATAYO - Unboxing of the new version of the TIP
17:10	17:30	Community roundtable & Q&A
17:30	17:40	Recognition of the most active community members
17:40	17:55	Closing & upcoming community events

Thank you (...and happy reading!)

*If there is one lesson that years of threat intelligence work have thought me, it is this:
good intelligence begins with the right questions.*

Massimo Giaino

Domande?

