NetEye

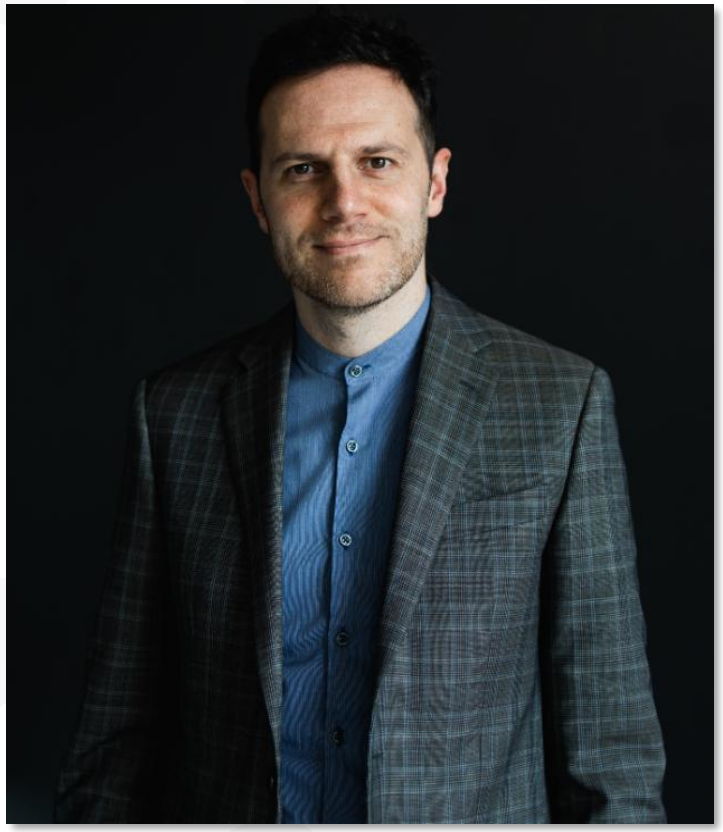
NETEYE CONFERENCE 2025

From Intelligence to Action

Embedding TI into Your Security Operations
(**Halloween Edition**)

Who Am I

- **Role:** Threat Intelligence Team Leader at the **Würth Group's Cyber Defense Center**
- **Communities:** deepdarkCTI, Curated Intelligence
- **Blog:** www.deepdakcti.com
- **My Linktree**



NetEye

The Intelligence-Action Gap

How many of you buy Threat Intelligence **feeds**?
How many feel you use them **effectively**?

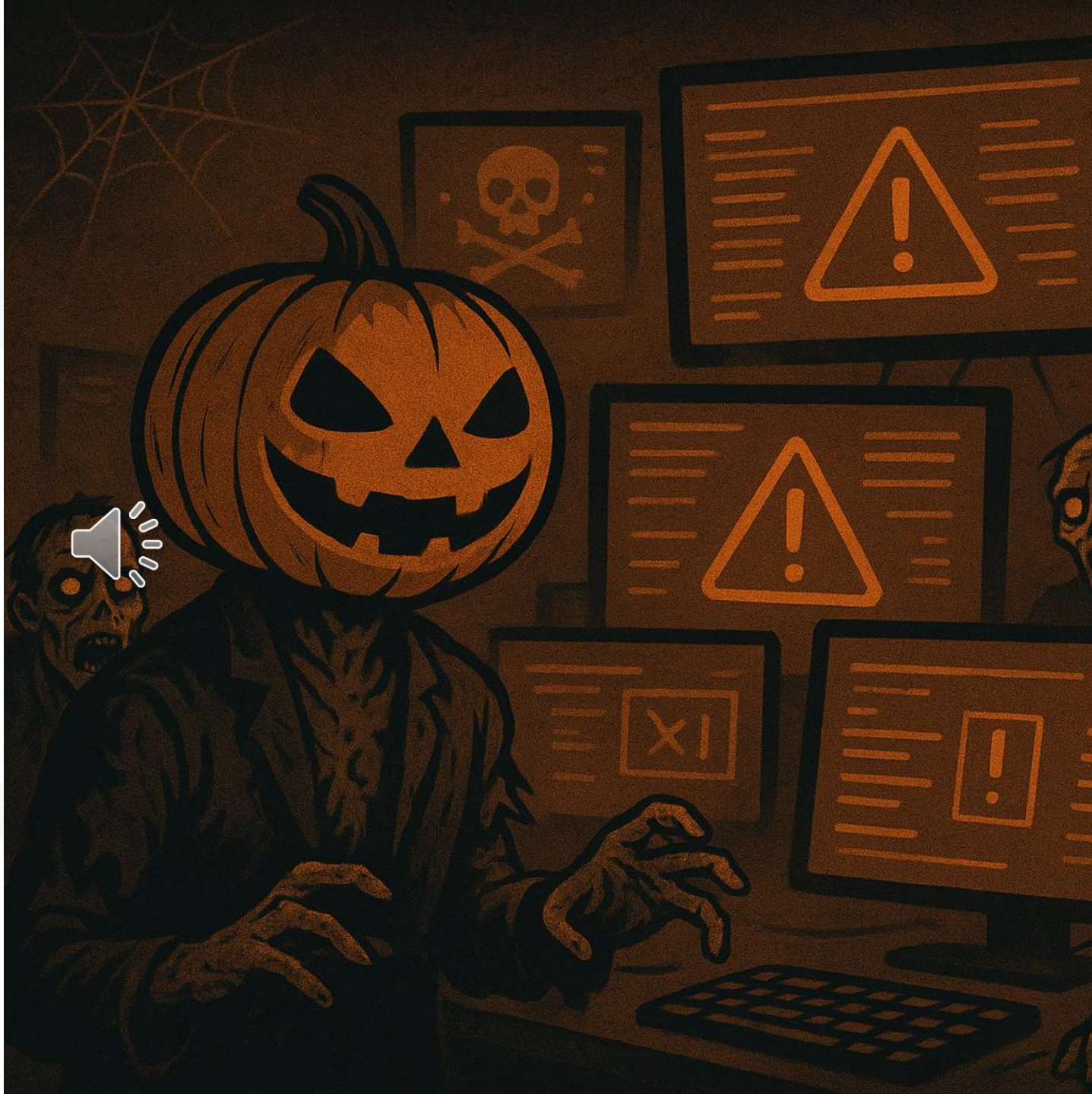
';--hibp?
SHODAN
censys
AbuseIPDB
VIRUSTOTAL
OPEN THREAT EXCHANGE
PhishTank
OPENCTI
ANY RUN
INTERACTIVE MALWARE ANALYSIS
THE HONEYNET PROJECT
GREYNOISE
SPAMHAUS

The Problem

Why Threat Intelligence often fails to deliver value?

- Too many **raw IOCs** → analyst overload
- **Feeds not integrated** into daily tools
- **Lack of context** for prioritization
- Business risk: **wasted spend** + **missed threats**

This is an analyst's nightmare!



NetEye

Threat Intelligence Acquisition Scenarios

(and related pros and cons)

	Subscription to TIP	Subscription to TIP + Managed Analysis	TI as Part of the SOC Service	Outsource TI Service (No TIP Ownership)	Hybrid Model (Int + Ext Collaboration)
DESCRIPTION	The company buys access to a TIP (e.g., SATAYO, Recorded Future, Google Threat Intelligence, Anomali, etc.) and its data feeds. The internal blue team or TI analysts handle ingestion, enrichment, and analysis.	The provider offers both the platform and human analysis (enrichment, contextualization, reporting).	The SOC includes a TI component (feeds, correlation rules, contextual reports).	A provider delivers reports, briefings, and IOCs without giving access to a platform (pure managed service).	The company owns a TIP and has an internal TI team but also consumes curated intelligence and support from external experts or ISACs.
PROS	Full control over data, sources, and workflows. Customizable correlation with internal telemetry (SIEM, EDR, etc.).	Fast maturity gain and no need to build a full internal TI team. Continuous flow of actionable intelligence.	Integrated detection and response; SOC can act immediately. Simplified management (single provider). Cost-effective for small/medium organizations.	Minimal setup effor; fully outsourced. Predictable cost structure. Suitable for organizations with low TI maturity.	Balanced control and scalability. Combines internal visibility with external context. Strong collaboration and resilience.
CONS	Requires skilled analysts and dedicated time. Costly in human resources and training. Risk of underusing the platform if internal maturity is low.	Limited customization of analysis priorities (depends). Dependence on the provider for insights. Integration with internal tools may be constrained.	Usually focused on operational TI only (indicators, alerts), less on strategic or tactical layers. May lack flexibility for custom threat research (depends).	No data ownership or integration capability. Difficult to validate or enrich information internally. Lower long-term knowledge growth.	Requires governance to avoid data duplication or conflicting sources. Potentially higher overall cost. Needs coordination between multiple actors.

satayo SEARCH ALL THINGS ABOUT YOUR ORG

+ SaaS and Managed

+ SOC Attacker Centric Service

NetEye

I'll take a guess...

Why Threat Intelligence often fails to deliver value?

Case 1
Situation: The SIEM sends an alert regarding **scan attempts** from an AWS IP.
SOC Analyst 1: *Ouch, this IP is doing some nasty things! Let's check AbuseIPDB!*
SOC Analyst 2: *Ouch, this IP (the same) is doing some nasty things! Let's check AbuseIPDB!*
SOC Analyst N: *Ouch, this IP (the same) is doing some nasty things! Let's check AbuseIPDB!*

Case 2
Situation: Scoop #1! New **data breach** involving a gazillion credentials! Run for cover!
SOC Analyst: *I suggest notify all customers, they should reset their user credentials immediately.*

Case 3
Situation: Scoop #2! Critical zero day allows RCE on **vendor X** firewall dashboard!
SOC Analyst: *I recommend temporarily downing the internet connectivity of **customer Y**.*

Case 4
Situation: The SIEM sends an alert regarding a recently created **typosquatting domain**.
SOC Analyst: *I suggest blocking all incoming and outgoing traffic for that domain.*

Want to know the correct analysis for these use cases? Follow the pumpkin!

https://www.neteye-blog.com/2025/10/neteye-conference-2025-the-correct-analysis-for-some-use-cases/

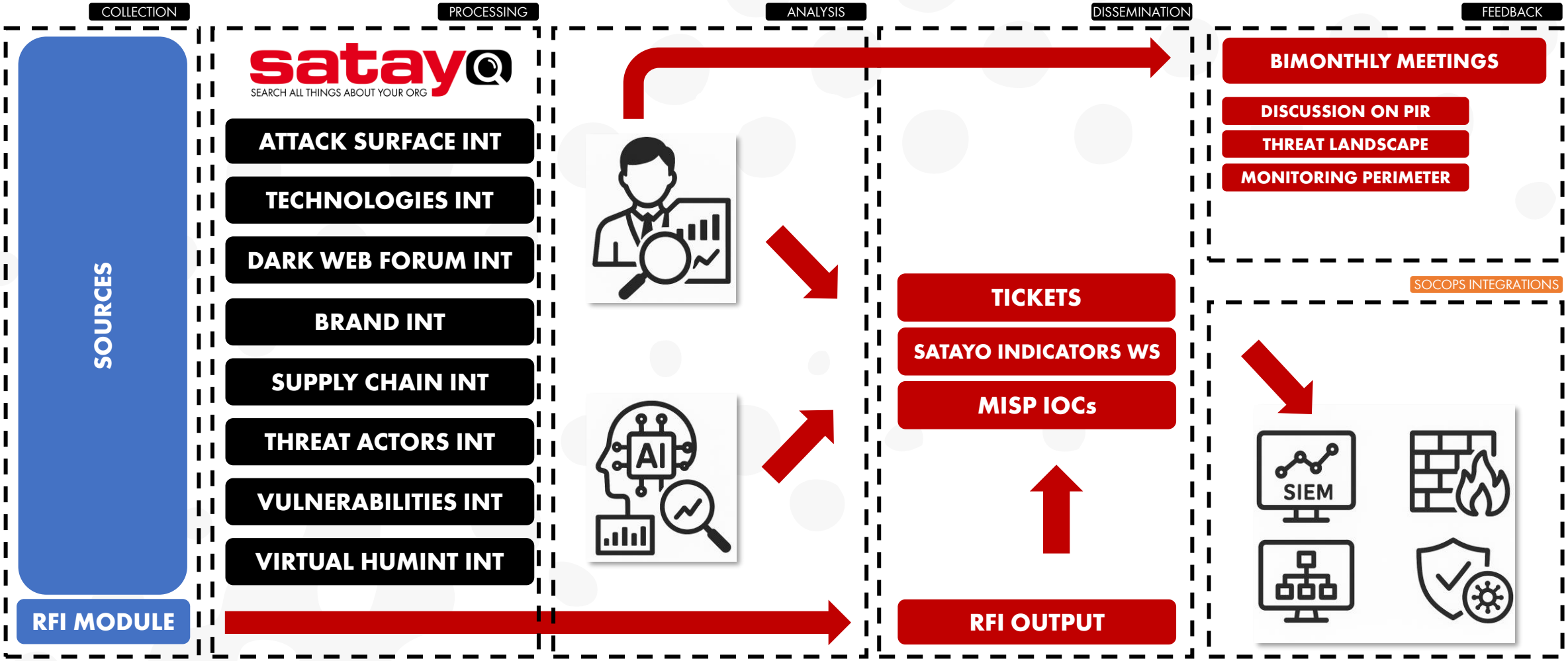
Vision: Intelligence That Works

Goal: Threat Intelligence **must be embedded** (at least) into:

- **SIEM** (better detection)
- **SOAR** (faster response)
- **EDR** (endpoint visibility & hunting)
- **Vulnerability Management** (smarter patching)

What intelligence do we produce and how we provide it?

(and therefore, what intelligence can the SOC Operations team integrate?)



NetEye

What intelligence do we produce and how we provide it?

(and therefore, what intelligence can the SOC Operations team integrate?)

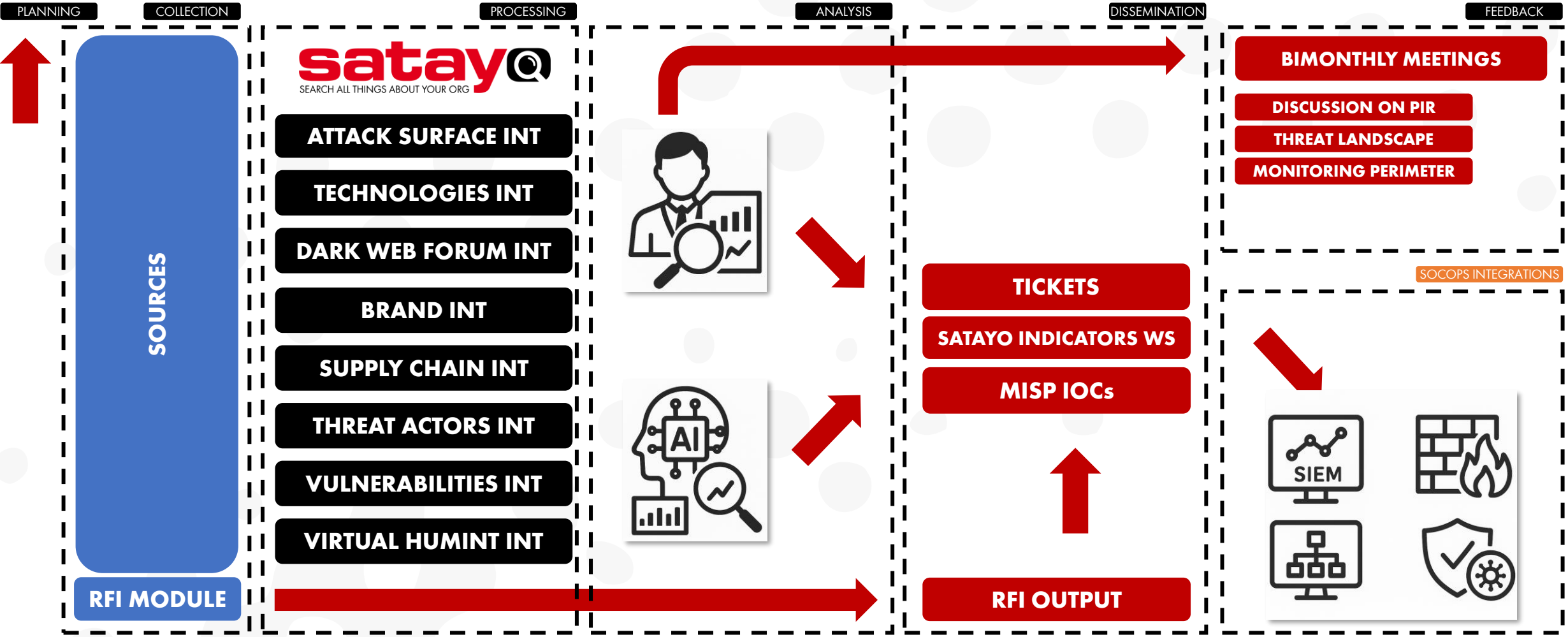
- COLLECTION
- PROCESSING
- ANALYSIS
- DISSEMINATION
- FEEDBACK

Question:
what did I forget?

NetEye

What intelligence do we produce and how we provide it?

(and therefore, what intelligence can the SOC Operations team integrate?)



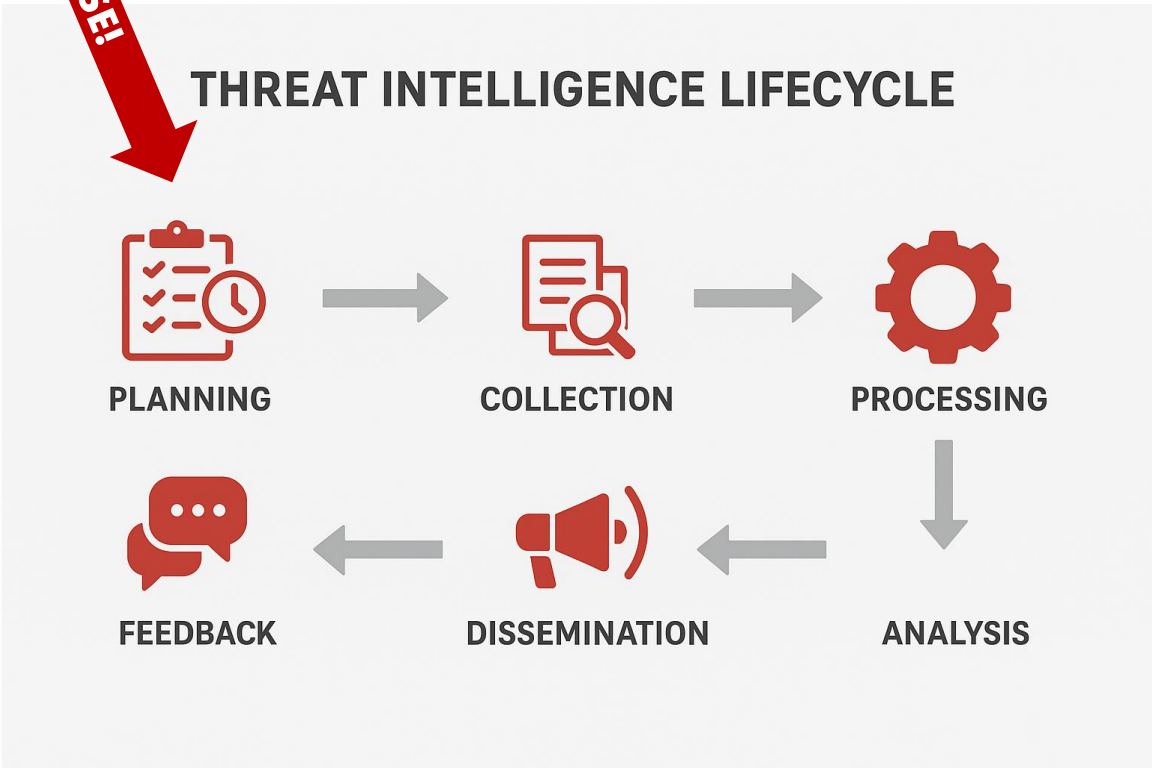
NetEye

Start by registering the PIRs

(aka Priority Intelligence Requirements)

- What are your organization's most critical business **processes**, **services**, **data**, or **assets**?
- Which **business units** or **subsidiaries** would have the highest operational or financial impact if disrupted by a cyberattack?
- Which types of **threats** or **threat actors** concern you the most?
- Are there specific **regions**, **industries**, or **technologies** you believe are being targeted that overlap with your organization's exposure?
- Have you experienced significant **incidents** in the past?
- What parts of your **infrastructure** or digital footprint are most exposed to **external threats**?
- Do you have **third parties** or **suppliers** whose compromise could significantly impact your operations?

SET PIRs IN THIS PHASE!



5 practical Use Cases

(this is where I show you that it's truly possible to integrate TI into Security Operations)

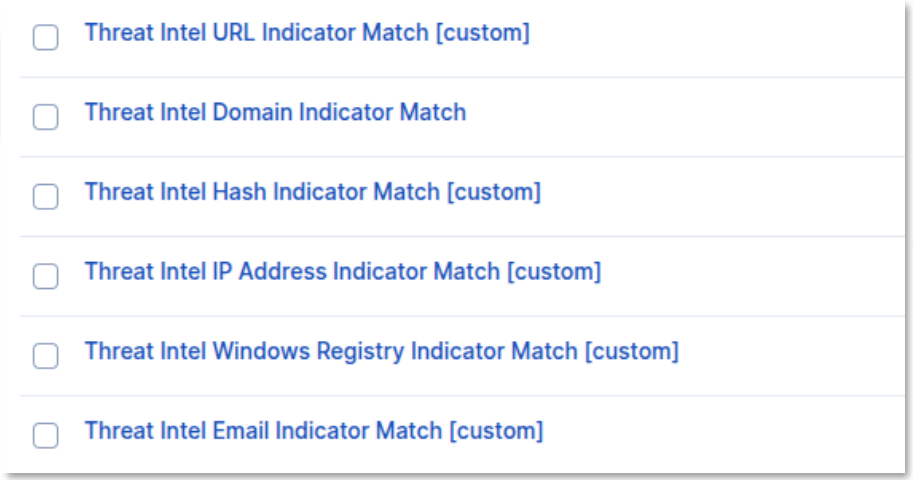
NetEye

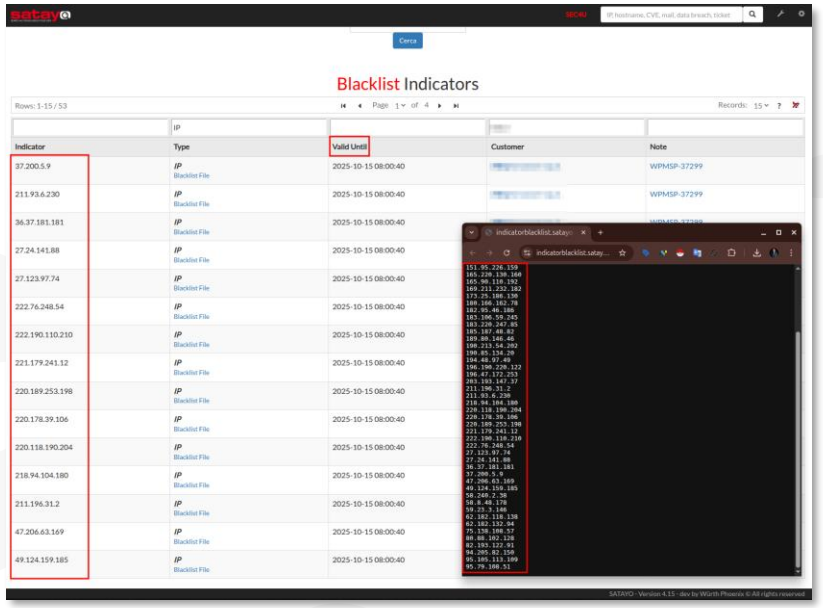
Case #1: Hunting with Context

Once we have the **MISP** platform integrated into the **SIEM**, we can manage **continuous hunting**!

Which indicators should be included in MISP?

- Indicators provided by paid feeds (usually higher quality)
- Indicators present on internal tickets managed by the SOC Operations team
- Indicators present on tickets managed by the Threat Intelligence team
- Indicators present on internal reports managed by the Incident Response team
- Indicators from publicly available reports





But for some scenarios, raw format may be the best choice!

Case #2: Vulnerability Management

How Threat Intelligence helps prioritize patching?

A Vulnerability Assessment (part of Vulnerability Management) process, by its very nature, is driven to produce a list of vulnerabilities.
Threat Intelligence can help us understand, for each vulnerability, whether:

- there are **exploits**
- it is **actively exploited**
- what are the **chances** of it being **exploited**
- there are **rumors** (even in underground environments)
- it is present on a system **exposed** to the **Internet**

The result: patching one (really) critical vulnerability often leads to fixing many other vulnerabilities.

tenable_sc.vulnerability.base_score	7.8
tenable_sc.vulnerability.severity.description	High Severity

Field	Value
risk.Vuln.Epss	93.32
risk.Vuln.Exploited_value	0
risk.Vuln.Exploits	true
risk.Vuln.External_ip	[50.58.[redacted], 50.59.[redacted]]
risk.Vuln.Kev	true
risk.Vuln.Remediation_priority	92
risk.Vuln.Seen_value	1
risk.Vuln.Timestamp_enrichment	Oct 9, 2025 @ 21:04:57.341

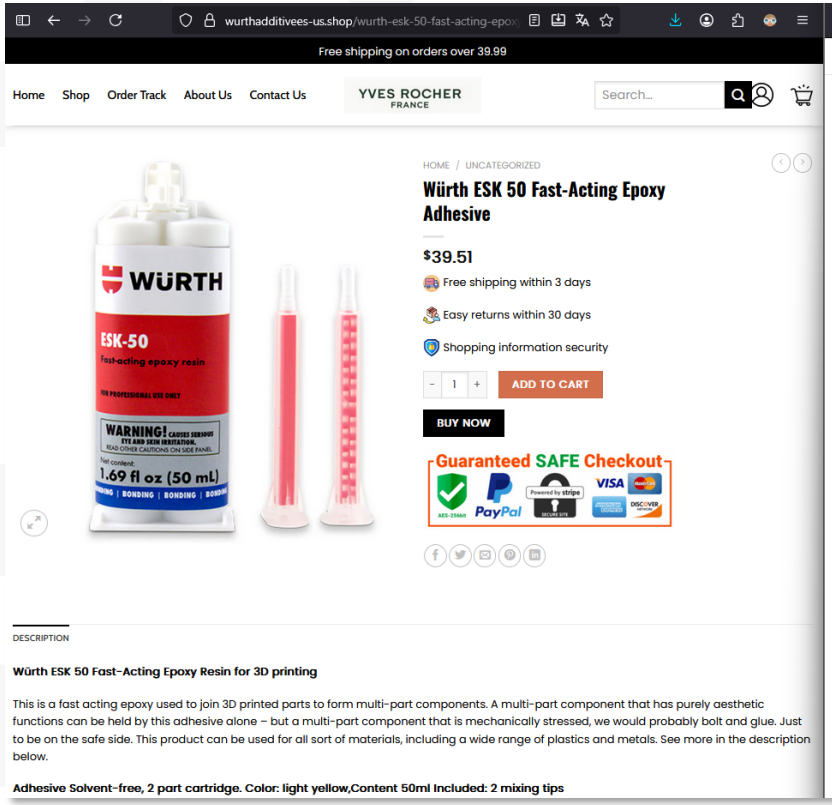
tenable

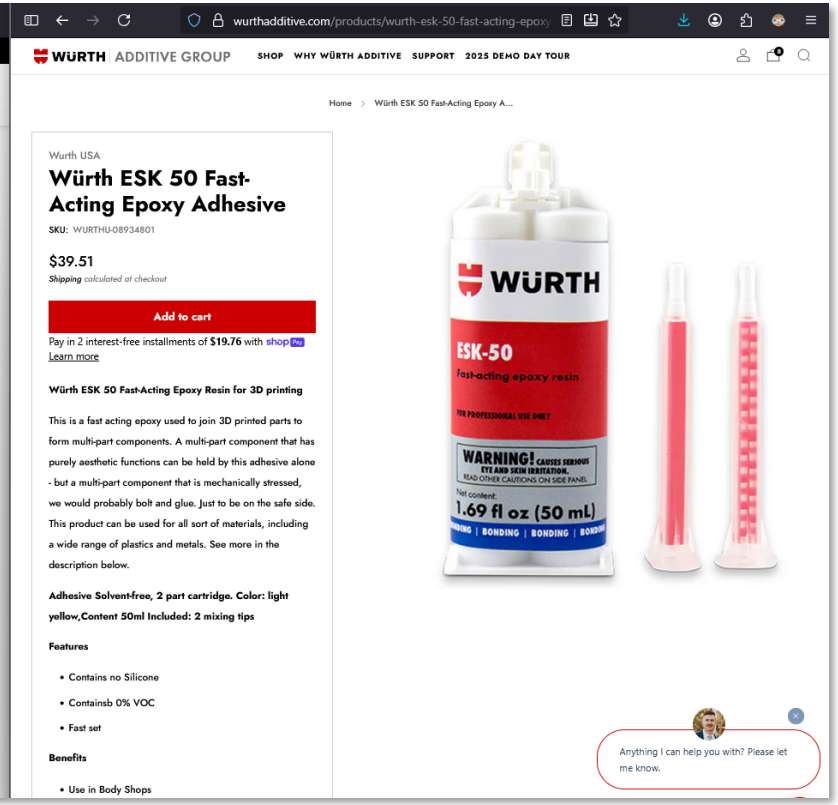
NetEye

Case #3: domain reported by TIP

MX	Blacklist	Time	Domain	Registrar	Registrant	Country	Creation date	Expire date	Last update date	Status
		7 days ago	wurthadditivees-us[.]shop							Resolved WPMSP-38578

satayQ
SEARCH ALL THINGS ABOUT YOUR ORG





NetEye

Case #3: domain reported by TIP

[102911] - domain_link | wurthadditivees-us.shop

Default | Contact Info | Managed Services | Consulting | Time Reporting | SAP Info | CYJD Time Reporting

[redacted] raised this request via **Jira**

View request in portal

Description

Summary

The domain wurthadditivees-us.shop was detected in SATAYO due to its similarity to **wurthadditive.com** on date 2025-10-15 07:13:00.
This domain was evaluated because it was registered recently.
We have determined this domain to be suspicious because it is provide explanation
Based on this, we classify the risk for your organization as high

It is necessary to proceed as soon as possible with the following mitigation measures:

- request a takedown with the registrar

The detailed mitigation steps are included at the bottom of the ticket, after the technical analysis.

Technical analysis

The domain in question was registered on **2025-10-13** through the registrar **Spaceship, Inc.**.

WHOIS

This domain doesn't have a WHOIS record associated.
However, using RDAP it was possible to retrieve some information:

```
Registration: 10/13/2025
Expiration: 10/13/2026
Last changed: 10/13/2025
```

Jira

Priority	Highest
Traffic Light Protocol	Amber+Strict
Sec4u_Indicator	wurthadditivees-us.shop
Sec4u_Blacklist_Indicator	wurthadditivees-us.shop

NetEye

Case #3: domain reported by TIP

[102911] - domain_link | wurthadditivees-us.shop

Event ID	13097
UUID	eabad218-999a-4382-89c9-1ed530b50a8b
Creator org	Würth
Owner org	Würth
Creator user	massimo.giaimo@wuerth-it.com
Protected Event (experimental)	Event is in unprotected mode. Switch to protected mode
Tags	phishing:action="take-down"
Date	2025-10-22
Threat Level	Low
Analysis	Initial
Distribution	This community only
Published	No (last published at 2025-10-22 07:09:14)
#Attributes	2 (0 Objects)
First recorded change	2025-10-22 07:06:20
Last change	2025-10-22 07:23:57

MISP Threat Sharing

Rule type	Indicator Match
Timeline template	Generic Threat Match Timeline
Indicator index patterns	logs-ti_*
Indicator filters	event.category: threat; event.kind: enrichment; event.type: indicator
Indicator index query	@timestamp >= "now-7d/d" and event.module: (threatintel or ti_*) and threat.indicator.url.domain:* and threat.indicator.type:"domain-name" and not labels.is_ioc_transform_source:"true" and misp.attribute.to_ids:"true"
Indicator index query language	KQL
Indicator mapping	(destination.registered_domain MATCHES threat.indicator.url.domain) OR (dns.question.registered_domain MATCHES threat.indicator.url.domain) OR (source.registered_domain MATCHES threat.indicator.url.domain) OR (source.domain MATCHES threat.indicator.url.domain) OR (server.domain MATCHES threat.indicator.url.domain) OR (destination.domain MATCHES threat.indicator.url.domain) OR (url.domain MATCHES threat.indicator.url.domain) OR (m365_defender.event.url_domain MATCHES threat.indicator.url.domain)

elastic

Date ↑	Context	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS
2025-10-22	c13...ba2	Network activity	domain	wurthadditivees-us.shop				✓			✓
2025-10-22	a3d...504	Internal reference	link	[redacted]				✓			☐

NetEye

Case #3: domain reported by TIP

DMCA Takedown Request – Unauthorized Use of Copyrighted Content by Fake Store - wurthadditivees-us[.]shop

3G

A: abuse@spaceship.com

Rispondi | Rispondi a tutti | Inoltra

mar 21/10/2025 11:11

Dear DMCA Agent,

we are WÜRTH-IT Security Operation Center https://www.wuerth-it.com/ and we are writing to notify you of a copyright infringement under the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512.
We are authorized to act on behalf of the owner of copyrighted material that is being used without permission on a website posing as a legitimate store.
This site is falsely advertising products using copyrighted content, and we can confirm it is a fraudulent fake shop.

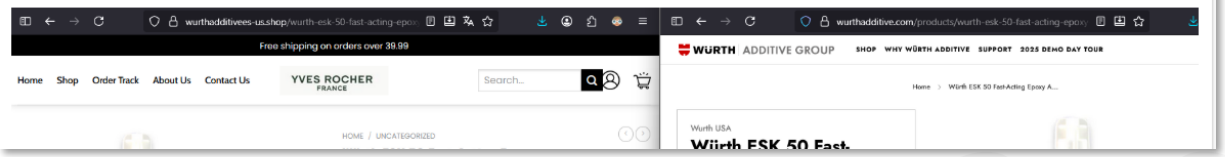
Copyrighted Work
The content being infringed includes:

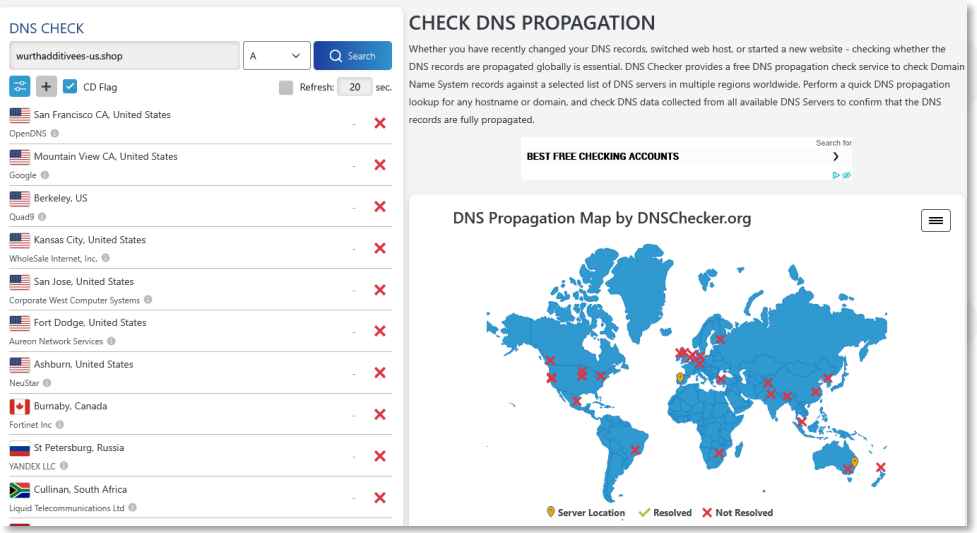
- Product images
- Descriptions
- Logos/branding
- Website layout or content

These are original works created and owned by Würth Additive Group, and are protected under copyright law.
You can find the original copyrighted content here:

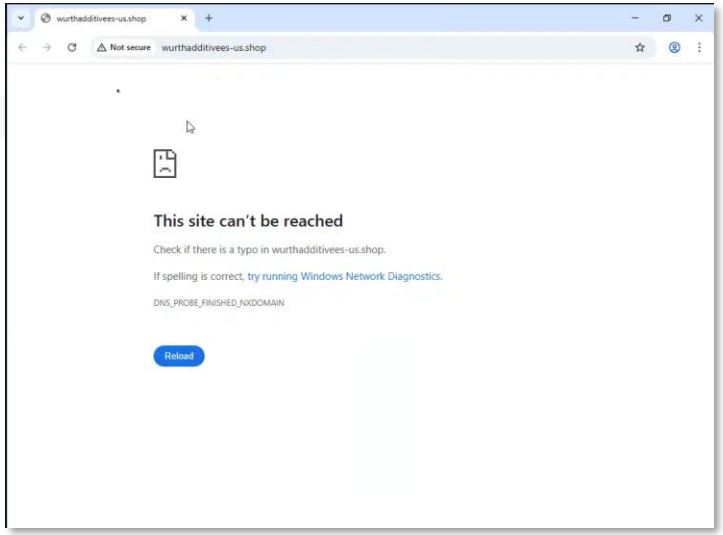
- https://wurthadditive.com/

Below a sample comparison between the fraudulent website (on the left) and the original one (on the right):





Is it always that simple?!
Oh, certainly not!

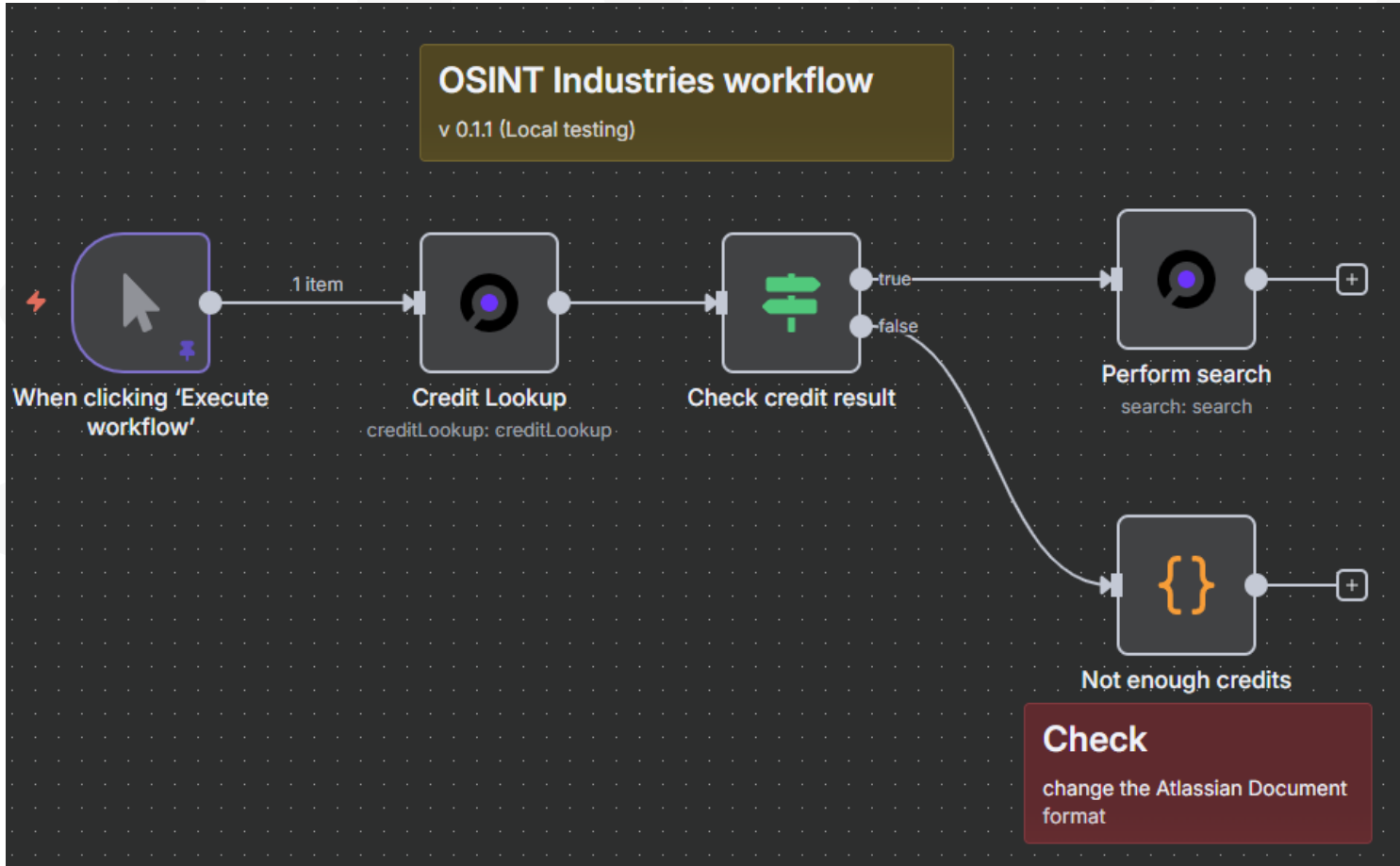


NetEye

Case #4: SOAR Automatic Response

How Threat Intelligence powers SOAR playbooks?

- Auto-block malicious IPs/domains
- Auto-quarantine suspicious endpoints
- Guided escalation (actor profiles, TTPs)
- Enriching an email account



n8n

NetEye

Case #4: SOAR Automatic Response

[150415] - (INT) - Office 365 Email Forwarding Rule | 84.18.[redacted] - Michael.[redacted]

Default | Contact Info | Managed Services | Consulting | Time Reporting

jsm.wpsoc.api raised this request via **Jira**
View request in portal

Description

OVERVIEW

Il SIEM NetEye ha segnalato la creazione di una regola di forwarding su Office 365.

Questa attività potrebbe indicare esfiltrazione di informazioni aziendali potenzialmente riservate e sensibili.

DETAILS

- Utente: `Michael.[redacted]`
- IP sorgente: `84.18.[redacted]`
- Regola di forwarding: `updateinboxrules`
- Timestamp: `Sep 4, 2025, 11:30:00 AM`

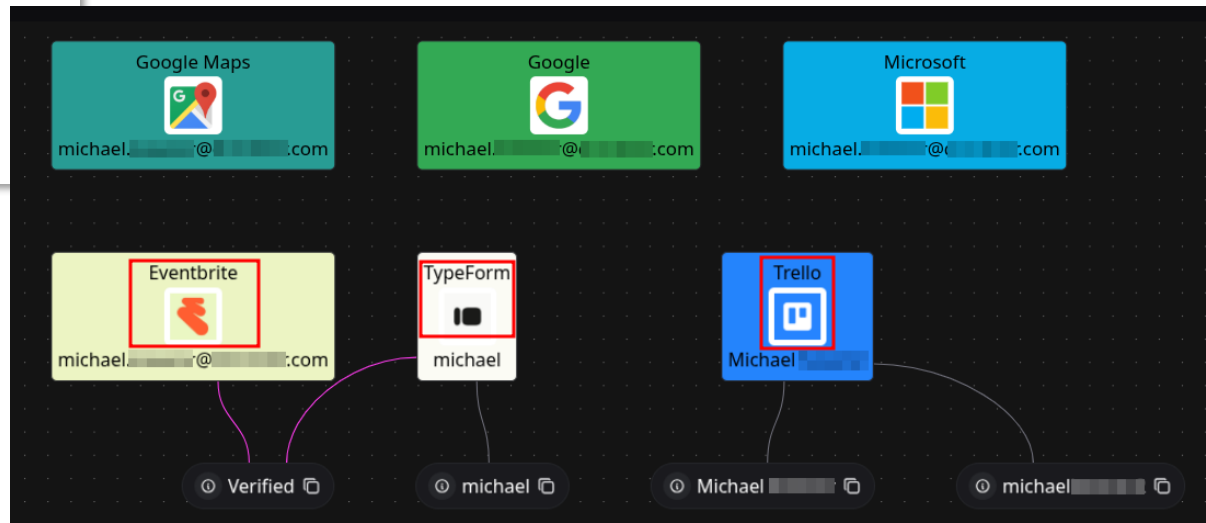
jsm.wpsoc.api September 4, 2025 at 12:24 PM Edited Internal note

michael.[redacted]@[redacted].com

SEARCH: Correlations found in OSINT Industries. See the PDF.

Creating preview...

export_michael...com.pdf
09 Oct 2025, 12:46 PM



Subsequent SOAR Workflows

If the set thresholds are triggered, I can, for example:

- reset the password
- disable the user

Case #5: ip detected by SIEM detection rule

Malicious Traffic blocked: Microsoft SharePoint CVE-2025-49704

Event ID	12361
UUID	37ea056a-7bc1-4008-b7ee-33f722df0a0e
Creator org	
Owner org	
Creator user	
Protected Event (experimental)	Event is in unprotected mode. Switch to protected mode
Tags	tlp:amber x PAP:AMBER x
Date	2025-07-23

2025-07-23*	4cd...4fe	Payload delivery	ip-src	34.53.105.114	tlp:amber x PAP:AMBER x	SOURCE IPs OF THE VULNERABILITY SCAN / MALICIOUS TRAFFIC TO OUR SERVERS. REQUESTS to: /_layouts/15/ToolPane.aspx	

MISP Threat Sharing

NetEye

Case #5: ip detected by SIEM detection rule

Medium 62
Low 21

Kerberos Brute Force Attempt 72
Potential Exploitation of CVE-2024-3094 - ... 39

Columns 17 | Sort fields 1 | 669 alerts | Updated 2 minutes ago
Fields | Grid view | Additional filters | Group alerts by: None

@timestamp	kibana.alert.threshold_result.terms.value	Rule	Assignees
Jul 22, 2025 @ 17:34:33.228		Attempts to Brute Force a ...	
Jul 23, 2025 @ 10:24:33.638		Attempts to Brute Force a ...	
Jul 23, 2025 @ 11:37:34.215	—	Threat Intel IP Address Indi...	
Jul 23, 2025 @ 11:37:34.217	—	Threat Intel IP Address Indi...	
Jul 23, 2025 @ 11:37:34.219	—	Threat Intel IP Address Indi...	
Jul 23, 2025 @ 11:37:34.221	—	Threat Intel IP Address Indi...	
Jul 23, 2025 @ 11:37:34.223	—	Threat Intel IP Address Indi...	
Jul 23, 2025 @ 11:37:34.225	—	Threat Intel IP Address Indi...	
Jul 23, 2025 @ 11:37:34.227	—	Threat Intel IP Address Indi...	
Jul 23, 2025 @ 11:37:34.229	—	Threat Intel IP Address Indi...	
Jul 23, 2025 @ 11:37:34.231	—	Threat Intel IP Address Indi...	
Jul 23, 2025 @ 11:37:34.233	—	Threat Intel IP Address Indi...	
Jul 23, 2025 @ 11:37:34.235	—	Threat Intel IP Address Indi...	
Jul 23, 2025 @ 11:37:34.237	—	Threat Intel IP Address Indi...	
Jul 24, 2025 @ 10:11:04.515	—	Windows Event Logs Clean	
Jul 24, 2025 @ 15:51:05.239	—	Windows Event Logs Clean	
Jul 24, 2025 @ 17:30:16.788		Kerberos Brute Force Atten	

Rows per page: 50 | 1 2 3 4 5 ... 14

High
Jul 23, 2025 @ 11:37:34.215
⚠ Threat Intel IP Address Indicator Match [custom]

Status: Closed | Risk score: 73 | Assignees | Notes: Add note

Overview | Table | JSON

About

Rule description — Show rule summary

This rule is triggered when an IP address indicator from the Threat Intel Filebeat module or integrations has a match against a network event. This version of the rule takes into account the MISP attribute to_ids.

Alert reason — Show full reason

network event with source 34.53.105.114:46325 destination :443, created high alert Threat Intel IP Address Indicator Match [custom].

Investigation

Show investigation guide

Highlighted fields

Field	Value
rule.name	OUTSIDE to
kibana.alert.rule.type	threat_match
destination.port	443
source.port	46325
kibana.alert.rule.parameters.threat_index	filebeat-*logs-ti_*

elastic

Jira

[152656] - (INT) - Threat Intel IP Address Indicator Match | 34.53.105.114 →

Create subtask | Investigate | Find resources | Link work item | Add form | Add PIR | Create | Start conversation | Send Email | Schedule

Default | Contact Info | Managed Services | Consulting | Time Reporting

jsm.wpsoc.api raised this request via Jira — Hide details
View request in portal

Description

OVERVIEW

Il SIEM NetEye attiva questa regola quando un indirizzo IP segnalato dal modulo Threat Intel di Filebeat o dalle integrazioni corrisponde a un evento di rete.

DETAILS

- Sorgente: `34.53.105.114`
- Destinazione.
- Port: `443`
- Action: `flow_terminated`
- Outcome: `Success`
- Timestamp: `Jul 23, 2025 @ 11:50:25.120`

ANALYSIS

L'alert è scattato a causa di una corrispondenza tra un indirizzo IP segnalato come potenzialmente malevolo dal modulo Threat Intel di Filebeat e un evento di rete rilevato dal sistema.

Nello specifico si tratta dell'IP `34.53.105.114` associato a `Google LLC`, che ha effettuato più 5 eventi verso l'IP interno

L'IP risulta segnalato come malevolo:

34.53.105.114 | Google LLC | AbuseIPDB

Request For Information

CTI Request for information
Are you requesting Cyber Threat Intelligence details about a specific threat, domain, IP, or suspicious activity?

Required fields are marked with an asterisk *

Raise this request on behalf of *

Massimo Giaimo (massimo.giaimo@wuerth-it.com)

Type of Information Requested *

Summary *

Known Details

Normal text

Provide any initial information already available about the threat

Priority Level *

Medium

Indicate the urgency of the request

Request Deadline *

e.g. 11/Sep/25

You need to make the SOC Operations team **confident** that they can ask the Threat Intelligence team questions! What questions?

- Threat Actor Profiling
- Malware Behavior Analysis
- Indicators of Attack (IoAs)
- Indicators of Compromise (IoCs)
- Tactics, Techniques and Procedures (TTPs)
- Mitigation Strategies
- Exploit or Vulnerability Details
- Domain Takedown Request

NetEye

So? The gran finale

(this is where I try to convince you that I've said useful things)

- Start with one assumption: Threat Intelligence within SOC Operations is **necessary**.
- Start by setting up **PIRs**.
- If your TI provider doesn't know what **PIRs** are, change providers.
- Threat Intelligence must be **actionable** (anyone who tells you otherwise is lying!
- Threat Intelligence findings must always be linked to a clear **Course of Action (CoA)**, often operational, sometimes strategic.
- There will always be someone who will question the usefulness of TI: ***measure it*** (but that's another topic, another talk is needed...) so you can disprove those who claim it.
- Acquire TI from those who are accustomed to producing TI, **not from those who are merely consumers** (MSP style).
- The more you consume TI (in the right way, of course), the more **convinced you** will be of its usefulness.
- Did I mention **PIRs** yet?

NetEye

Thank you!

Producing actionable intelligence must be the mindset that every Threat Intelligence analyst must set as their primary objective.

Massimo Giaimo aka fastfire

FollowThePumpkin2025

https://secureshare.wuerth-phoenix.com/s/zzAr7diXsgSEZDn

NetEye