Sentinel's Shield

Unleashing Threat Intelligence with Microsoft Defender

Your weatherman of duty

Ronny de Jong
Security Technical Specialist, Microsoft
CCSP, CISSP

ex Microsoft MVP: Enterprise Mobility

Contact Me
Twitter @ronnydejong
LinkedIn linkedin.com/in/ronnydejong/
Mail ronnydejong@microsoft.com

BBQ | CrossFit | F1 | Family time

Agenda

- Entering the digital battleground, where Threat Intelligence emerges as our beacon
- Decode the cryptic language of threats using Threat Intelligence
- Cybersecurity forecast: Stay ahead of potential storms
- Next steps & Key Takeaways

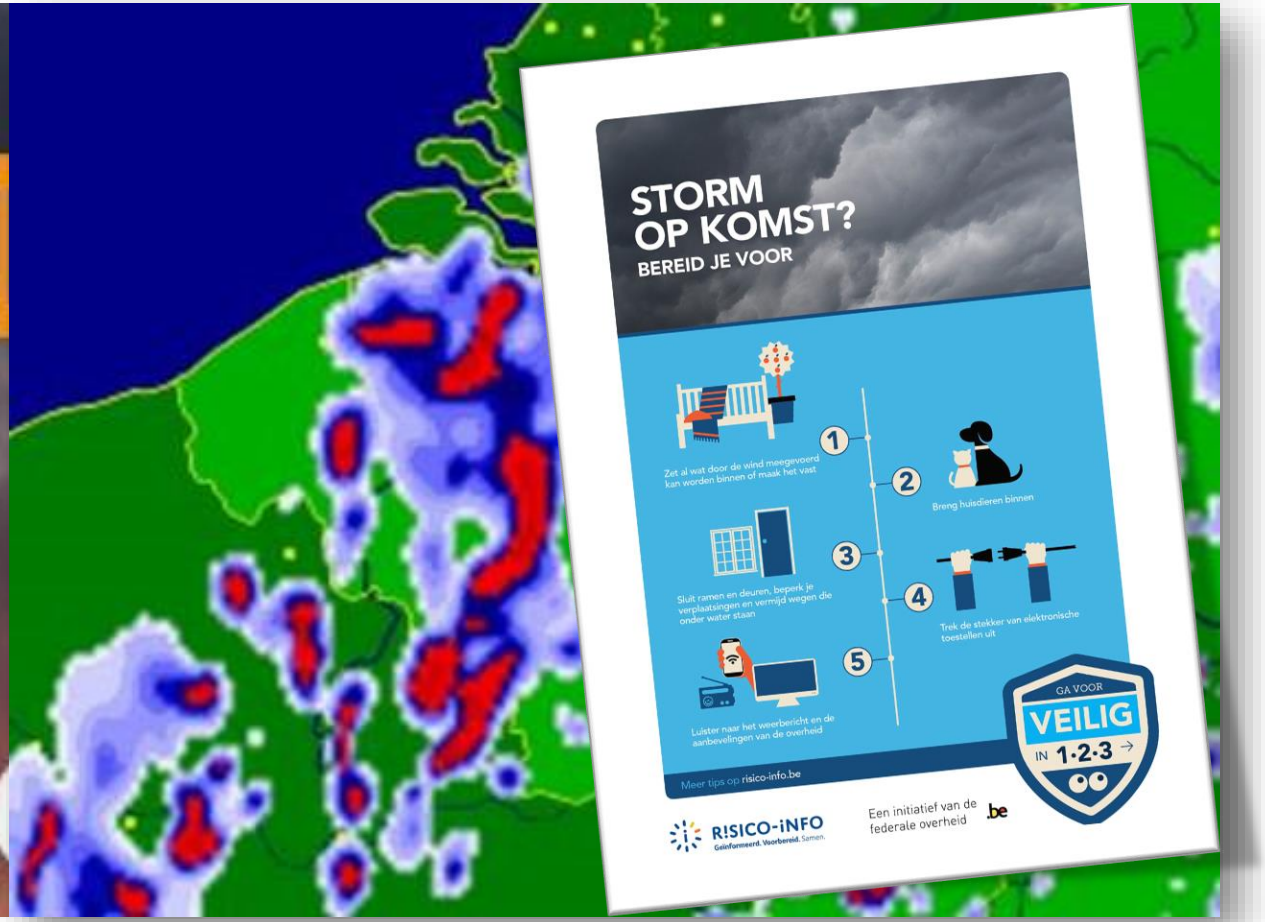
Welcome to the carnival of Threat Intelligence

RiskIQ
OSINT
PassiveDNS
JARM
TIP


IoC
FVEY
TTP
SONAR
MISP
ISAC
YARA

Threat intelligence…

…is the foundation of your organization's defense



Without the right intelligence you're falling short

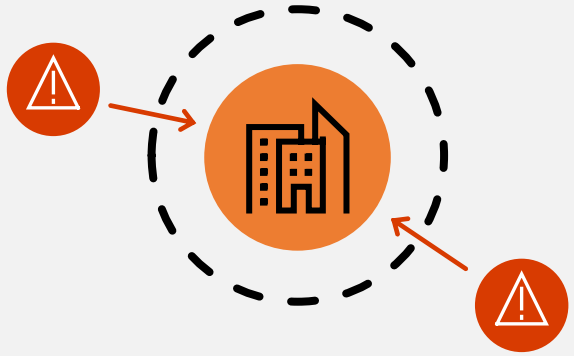
Many organizations are unable to:

Quickly remediate threats

They are too late to detect and respond to threats because their threat intelligence does not provide visibility across their entire attack surface

Effectively integrate TI with security tools

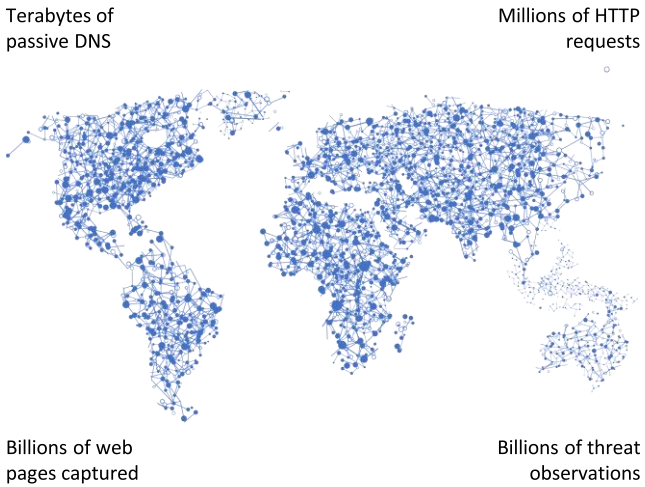
Their TI does not integrate or doesn't work well with their existing tools and workflows



Understand attackers

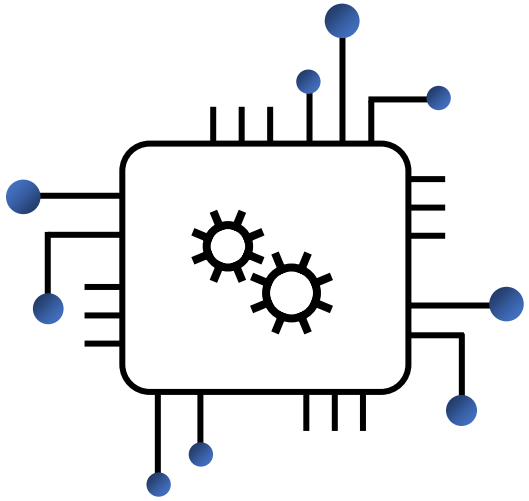
They are breached because they their intel is stale, and they lack understanding of who their attackers are and how they might exploit them

Threat Intelligence at glance



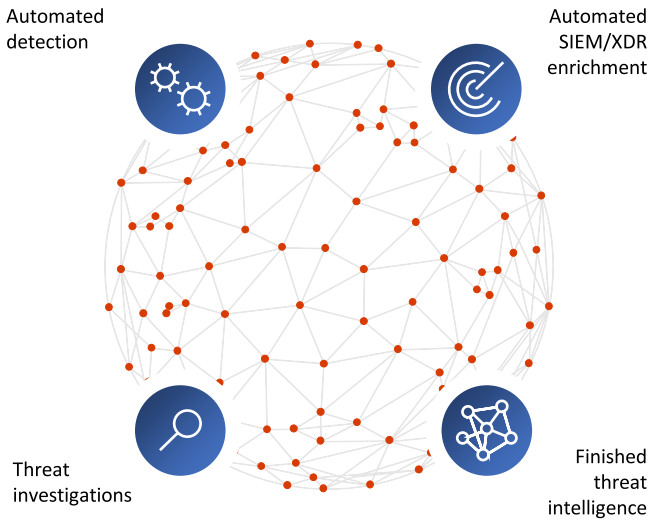
Advanced internet reconnaissance

Advanced global collection network with crawlers, sensors



Analysis

Data science, machine learning, security research, and threat intelligence



Dynamic threat intelligence

Reveals adversary infrastructure connections to unmask attackers and their tools

Why threat hunting?

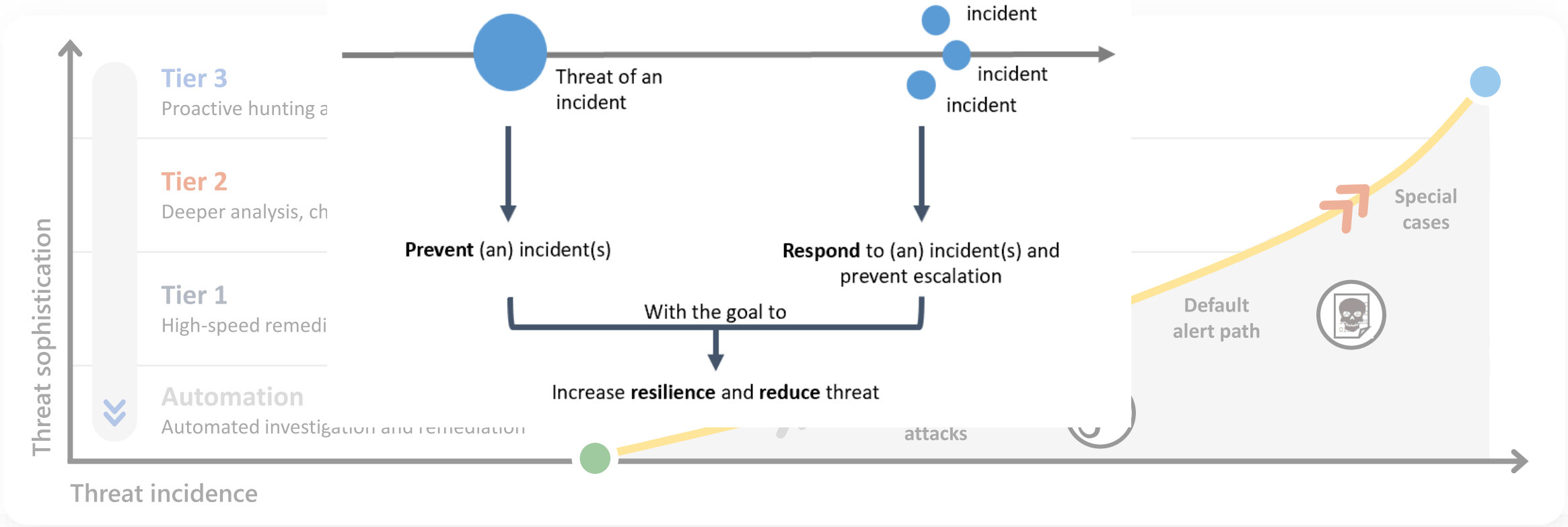
Where does Defender Threat Intelligence help?

Traditional cybersecurity is reactive

SOCs can be classified into a three-tier model when it comes to addressing unknown threats. Most organizations' responses operates in reactive tiers—automation, tier 1, and tier 2.

Threat Hunting is proactive

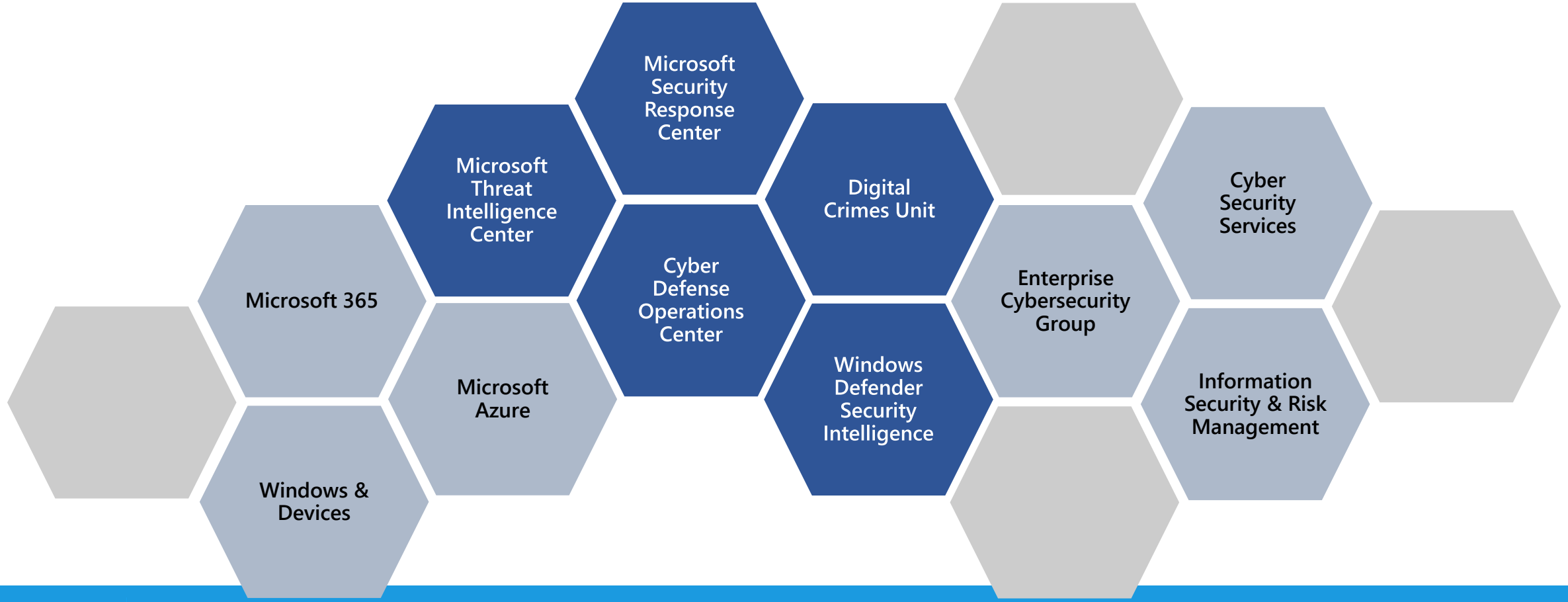
Threat hunting allows organizations to proactively mitigate threats. Analysts leverage specialized data and platforms to hunt a threat in totality. This process enriches lower response tiers, while reducing future incidents and breaches[1].



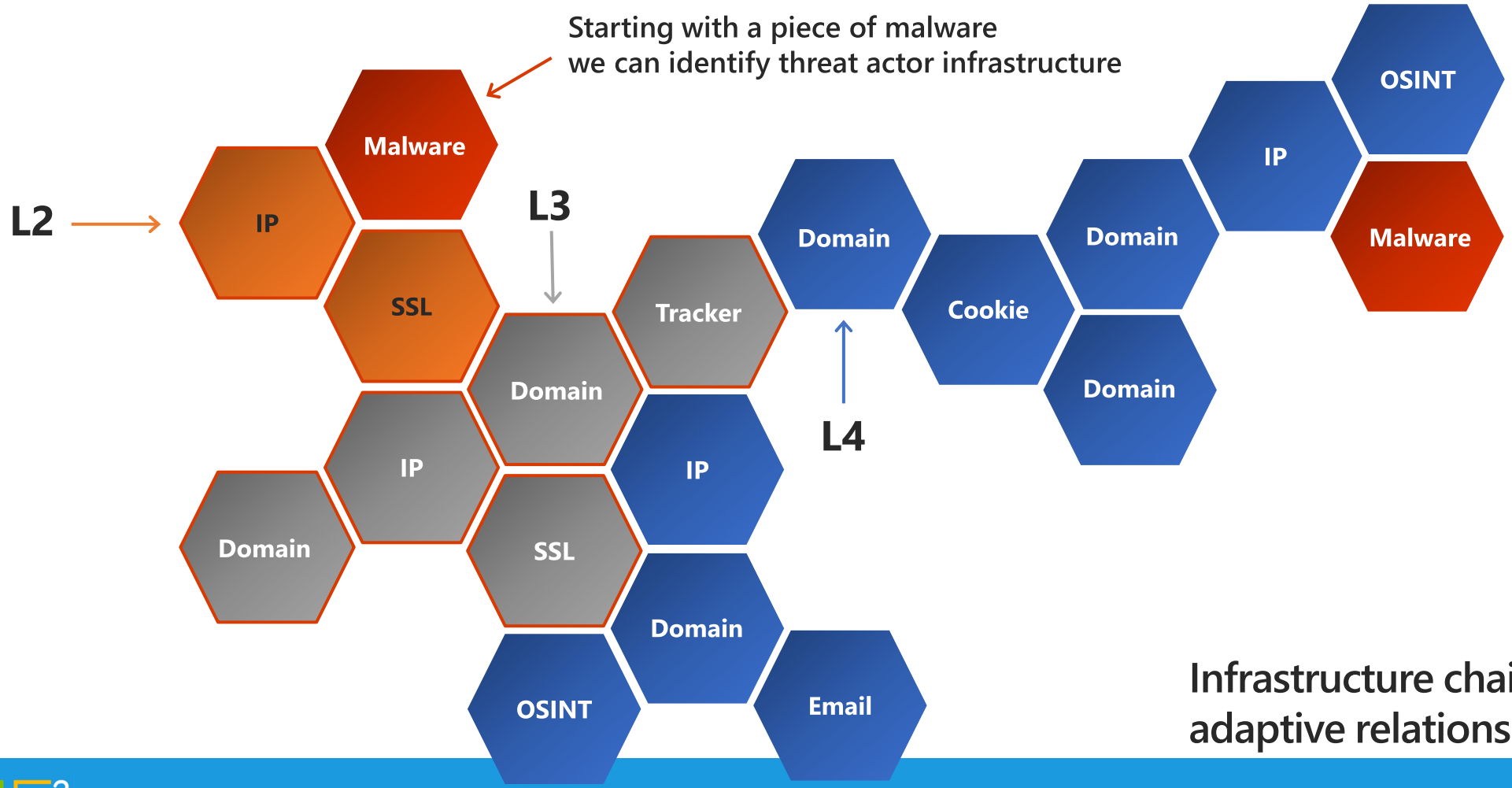
[1] https://www.microsoft.com/en-us/security/blog/2020/03/10/threat-hunting-part-1-why-your-soc-needs-a-proactive-hunting-team/

Intelligence: Working Together

Using intelligence gained across our vast digital estate, Microsoft security teams work together to secure all our cloud platforms



Understanding the adversary is the first step to keeping an organization safe



Infrastructure chaining™
adaptive relationship graphing

Agenda

- Entering the digital battleground, where Threat Intelligence emerges as our beacon
- Decode the cryptic language of threats using Threat Intelligence
- Cybersecurity forecast: Stay ahead of potential storms
- Next steps & Key Takeaways

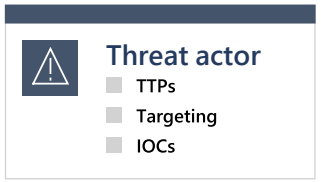
Microsoft Defender Threat Intelligence

Definitive source for quality insights that protect the world from cyberthreats

MDTI is the “encyclopedia" for Microsoft Threat Intelligence, enabling an intel-led approach to security

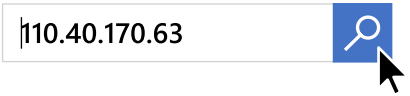
Keep updated with finished intelligence

The TI and Threat research that powers Microsoft Security products are made directly available to customers via an expansive content library and investigative workbench



Hunt on raw intelligence

Defenders can query Microsoft TI manually or at scale via an API to learn everything they need about any threat infrastructure



Microsoft threat intelligence

65 trillion daily signals **+** **8,500** researchers and experts

DEMO #1

Navigate through the cybersecurity forecast

Integrate MDTI with your tools and workflows

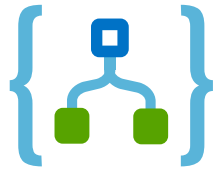
Enhancing protection, detection, and response

- MDTI Sentinel Data Connector
- MDTI Sentinel Analytics rules
- MDTI Enrichment Playbook
- MDTI API (must be licensed)

MDTI Sentinel Connector

MDTI Analytics rules

MDTI API



MDTI Playbooks

Integrate to enhance SIEM + XDR

Make your security solutions and workflows even more powerful

- Automatically enrich incidents with hyper-relevant threat intel and deep knowledge of threat infrastructure
- Automatically detect threats and threat tooling that matters most to your organization
- Automate workflows to scale your response to threats and help your team punch above its weight

DEMO #2

Preventing potential cyber hurricanes before they make landfall.

Agenda

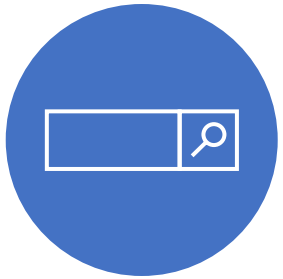
- Entering the digital battleground, where Threat Intelligence emerges as our beacon
- Decode the cryptic language of threats using Threat Intelligence
- Cybersecurity forecast: Stay ahead of potential storms
- Next steps & Key Takeaways

DEMO #3

Uncovering the secrets to orchestrating a robust response to cyber threats.

Raw threat intelligence

Build out your own hyper-relevant intelligence



- Develop hyper-relevant intel that helps you understand the most critical threats to your organization
- Global-scale observations of the entire internet as it evolves. See how threat infrastructures are connected
- Inoculate your organization from another attack by proactively blocking related infrastructure

DEMO #4

Enrichment through by combining raw cybersecurity data points

Next steps

- **Deploy Sentinel MDTI Data Connector**
  - Enable MDTI Analytic Rules
  - Add additional data sources (CEF, DNS, Syslog, Azure- & Office Activity logs)
- **Incident enrichment via automation**
  - Deploy MDTI Playbooks
    - https://aka.ms/mdti-solutions
  - Configure Watchlist Task Repository
    - https://aka.ms/mdti-task-repository
- **Enhanced scenarios**
  - Combining 3rd party data for new insights and thus new use-cases

Key Takeaways

- **Enhanced Cyber Defense.** Crucial information to strengthen an organization's cyber defense capabilities, proactively build defenses against emerging threats.
- **Uncovering Threat Actors.** Analyzing data related to their tactics, techniques, and procedures (TTPs), enabling accurate predictions and preventive measures.
- **Improved Decision-Making.** By revealing adversarial motives and helping analysts understand the threat actor's decision-making process.
- **Streamlined Response.** Staying ahead of threat actors, respond faster to incidents, reducing the impact of cyberattacks.

Thank you!

Ronny de Jong
Security Technical Specialist
Microsoft