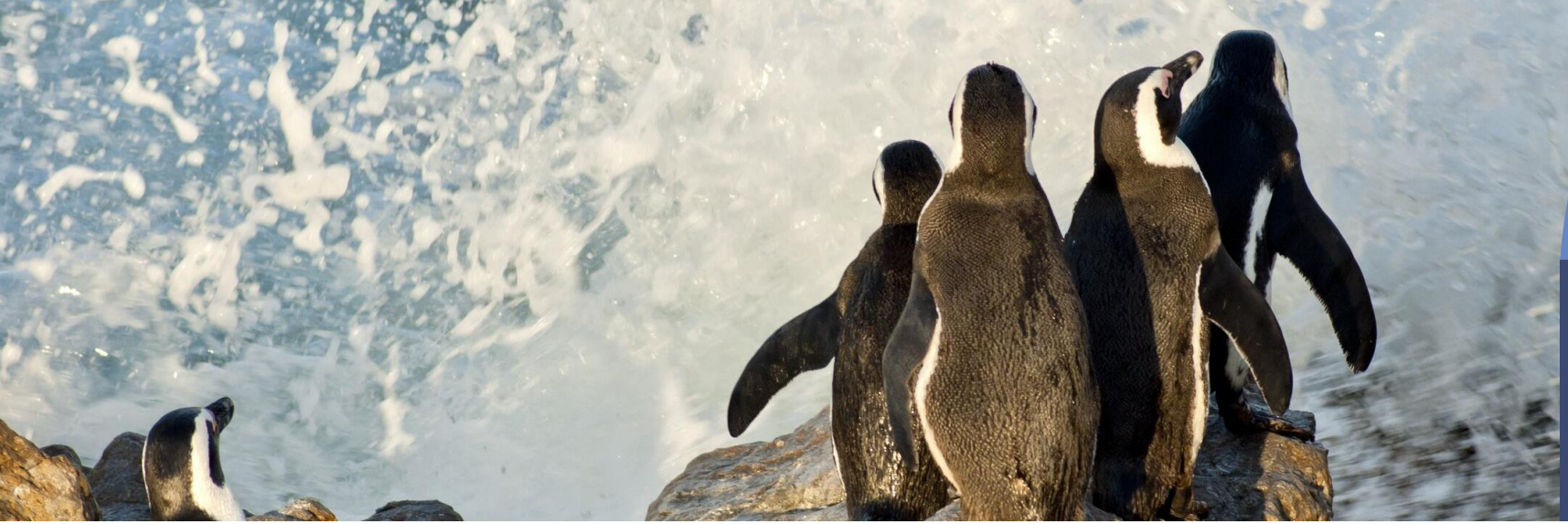


情 報 種 別 ：秘密(関係者限り)
会　社　名 ： NTT DATA Group Corp.
情報所有者 ： サイバーセキュリティ技術部

NTT DATA

IoC LIGHT

～ Lifecycle of Indicators: Gathering, Handling, and Termination ～

Jan 21st, 2025

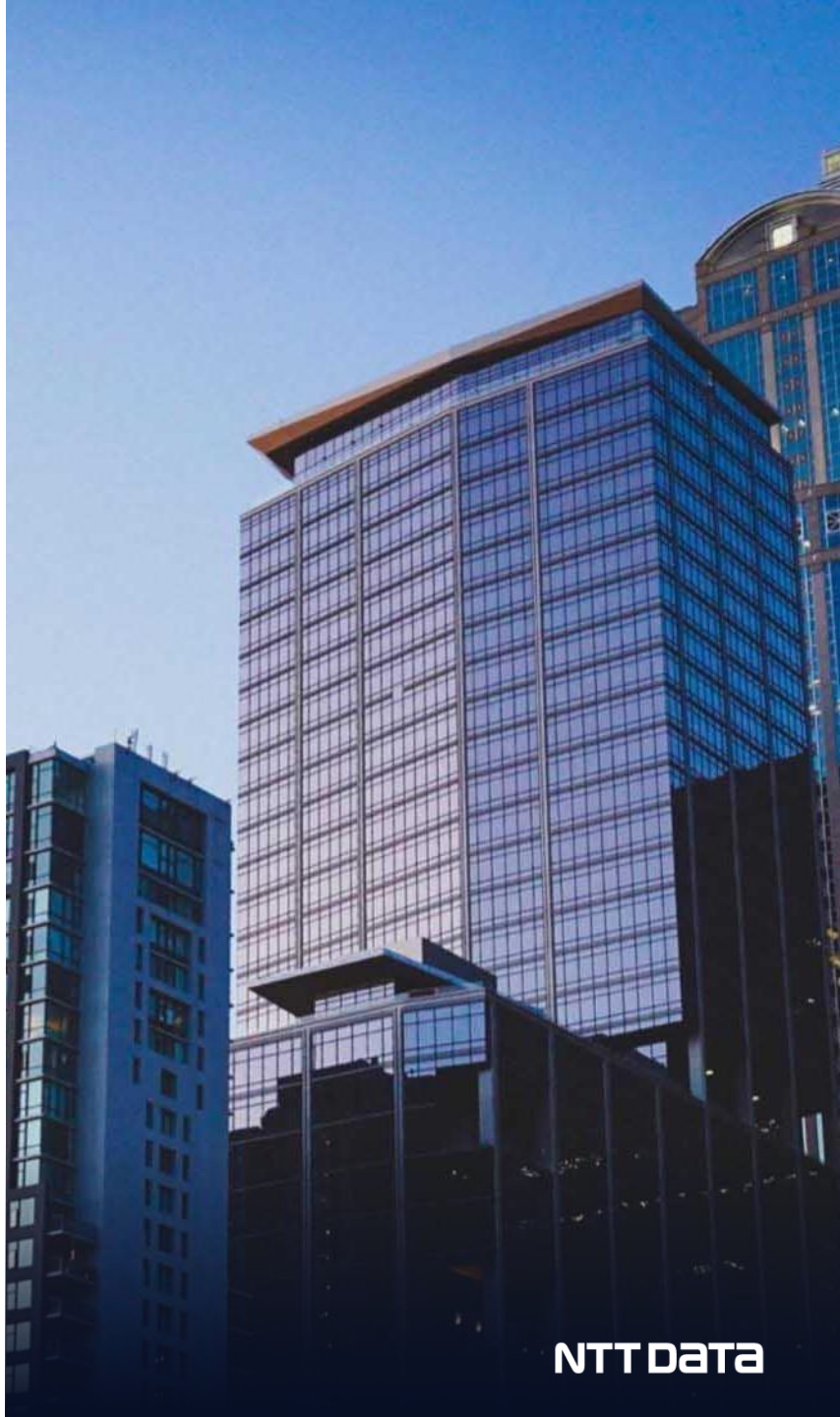
Yusuke Nakajima | NTTDATA-CERT | Cloud & Infrastructure Group | NTT DATA Group Corporation

© 2024 NTT DATA Group Corporation

NTT DATA

Agenda

1. whoami
2. Introduction
3. Two Challenges in IoCs Management and Approaches
4. IoCs Prioritization Criteria
5. IoCs Lifecycle Model
6. Conclusion

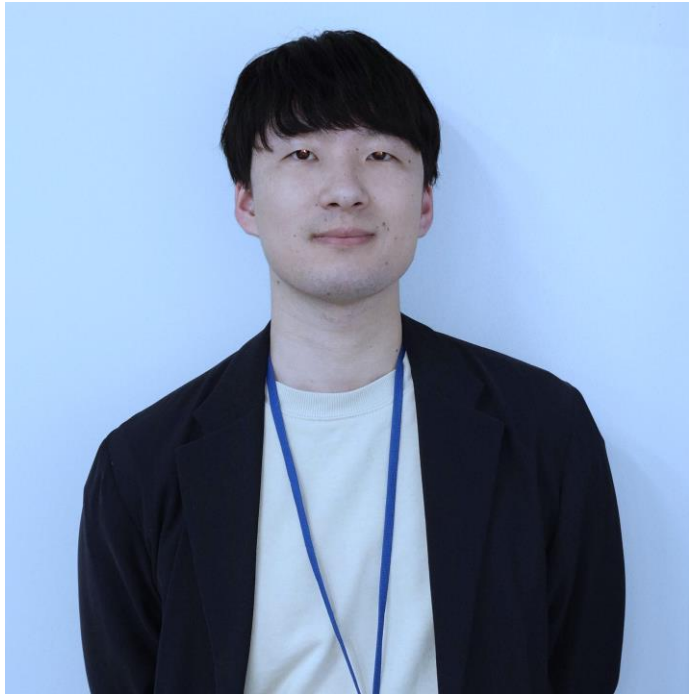


© 2024 NTT DATA GROUP Corporation

whoami

TLP:CLEAR

- Name: Yusuke Nakajima
- Background:
  - ✓ Joined NTT DATA Group in 2019, focused on providing image processing and NLP solutions
  - ✓ Transferred to NTTDATA-CERT in April 2023, handling incident response, IoC operations, and AI-driven CSIRT improvements
  - ✓ Interested in offensive security, including C2 framework development, open-source vulnerability research, and bug bounty programs

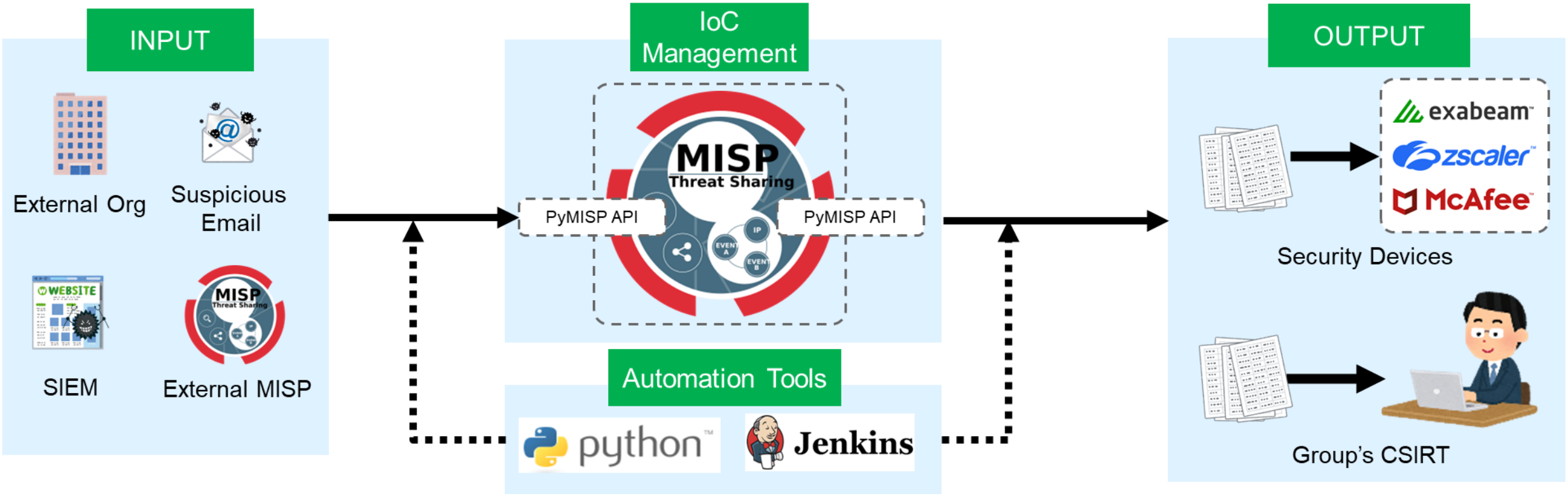


© 2024 NTT DATA Group Corporation

Introduction

TLP:CLEAR

- Performed real-time IoC collection, processing, and distribution using MISP as our core threat intelligence platform.
- Streamlined IoCs handling and quickly integrated new IoC sources. During the Emotet outbreak, **this approach allowed us to prevent incidents proactively.**



© 2024 NTT DATA Group Corporation

NTT DATA

Two Challenges in IoC Management and Our Approaches

TLP:CLEAR

- Threat trends evolve daily, requiring regular integration of new IoCs.
- Identified two key challenges in IoC management during this process.

1. IoC registration limits on security devices pose a significant challenge, as failing to filter out low-risk or outdated IoCs can **prevent the timely registration of high-risk, emerging threats, leaving critical gaps in defense（IoC Capacity Constraints）**

2. Retaining outdated IoCs increases false positives, leading to **alert fatigue and operational inefficiencies in SOC teams（False Positive Fatigue）**

© 2024 NTT DATA Group Corporation

Two Challenges in IoC Management and Our Approaches

TLP:CLEAR

- Our approaches to address these challenges are as follows:

No	Challenges	Approaches
1	IoC Capacity Constraints	**IoCs Prioritization Criteria** • Analyze IoCs to identify threats relevant to our organization • Categorize IoCs into four priority levels and collect only high-priority IoCs
2	False Positive Fatigue	**IoCs Lifecycle Model** • Develop removal criteria based on quantitative metrics, not qualitative metrics • Ensuring low-risk IoCs are systematically deleted from security devices such as FW, SIEM and so on

© 2024 NTT DATA Group Corporation

NTT DATA

IoCs Prioritization Criteria

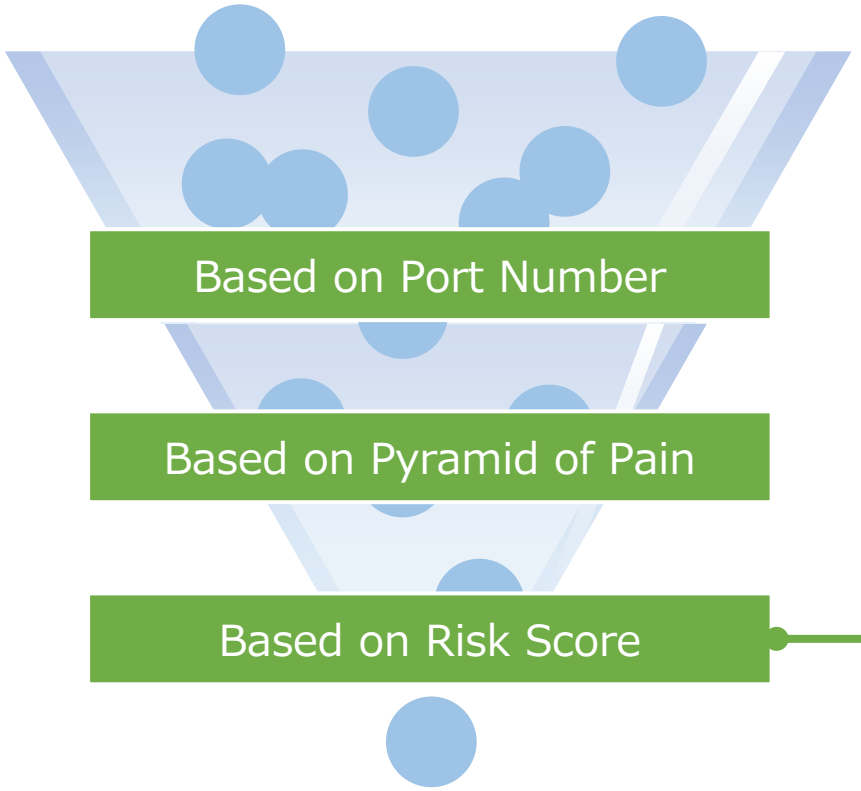
© 2024 NTT DATA Group Corporation

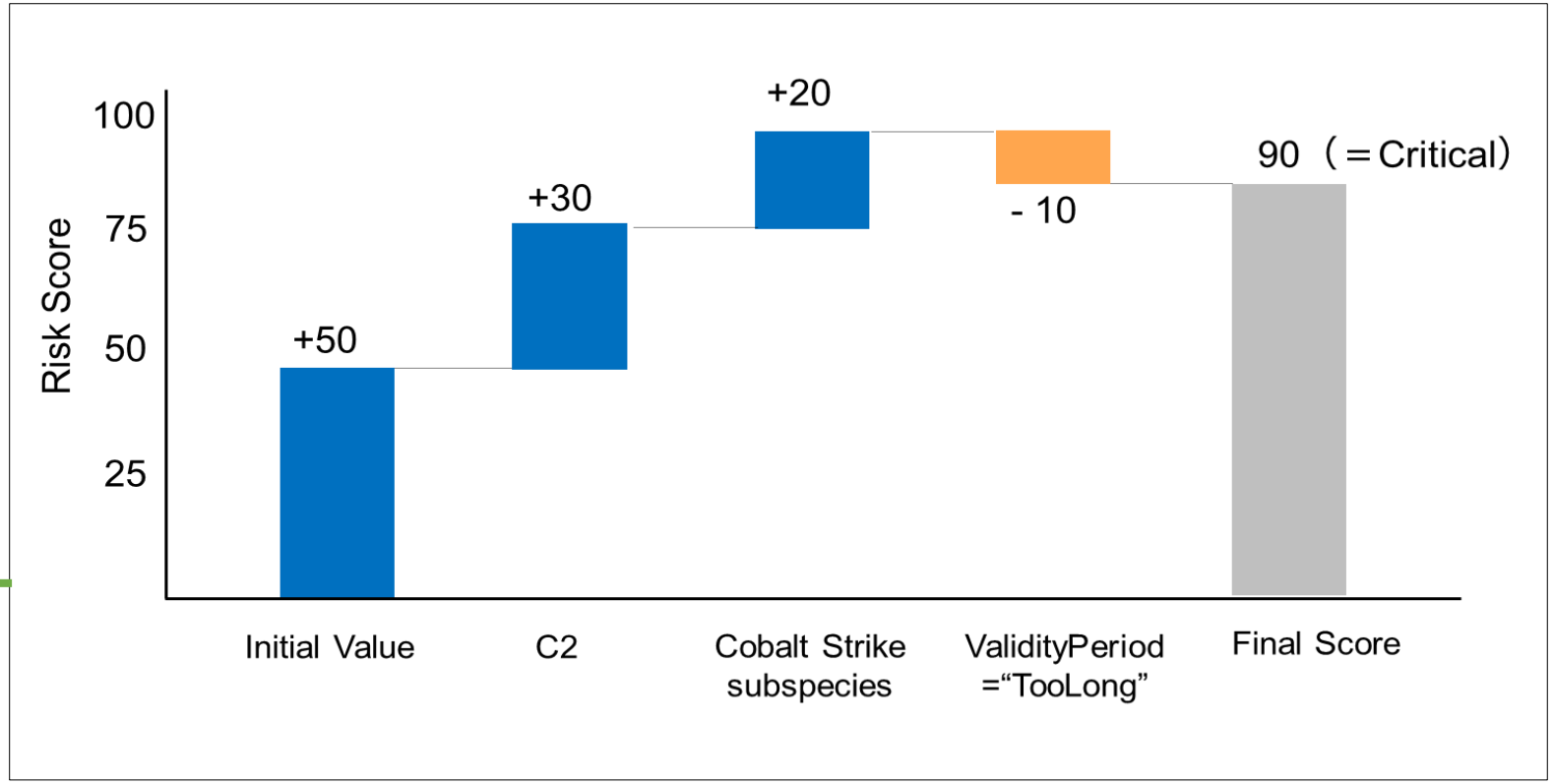
IoCs Prioritization Criteria

TLP:CLEAR

Overview

- Filtered a large volume of IoCs based on three key criteria: port number, Pyramid of Pain, and custom risk score.
- The Risk Score represents the **sophistication level of the attacker associated with the IoCs**





© 2024 NTT DATA Group Corporation

NTT DATA

IoCs Prioritization Criteria

TLP:CLEAR

Analysis of Our Security Environment（1/4）

- Security environment aligned with the Cyber Security Framework (CSF).
- External red team assessments confirmed that breaching our environment is challenging.
- Focus shifted to collecting IoCs related to advanced attackers, given **the low risk from unsophisticated threats.**

© 2024 NTT DATA Group Corporation

IoCs Prioritization Criteria

TLP:CLEAR

Analysis of Our Security Environment（2/4）

- Established a 24/7 SOC team focused on EDR solutions.
- Acknowledged **limitations of EDR in detecting C2 communications and data exfiltration.**
- **Prioritized C2 detection** as a key focus in our security strategy.

	EDR1		EDR2		EDR3		AV	
Abuse vector	Cobalt	Sliver	Cobalt	Sliver	Cobalt	Sliver	Cobalt	Sliver
C&C channel								
Open SOCKS tunnel, e.g. for Network scanning								
Data exfiltration								
KeyLogger								

Detected
Undetected

Source: [D1T1 - EDR Evasion Primer for Red Teamers - Karsten Nohl & Jorge Gimenez.pdf]

© 2024 NTT DATA Group Corporation

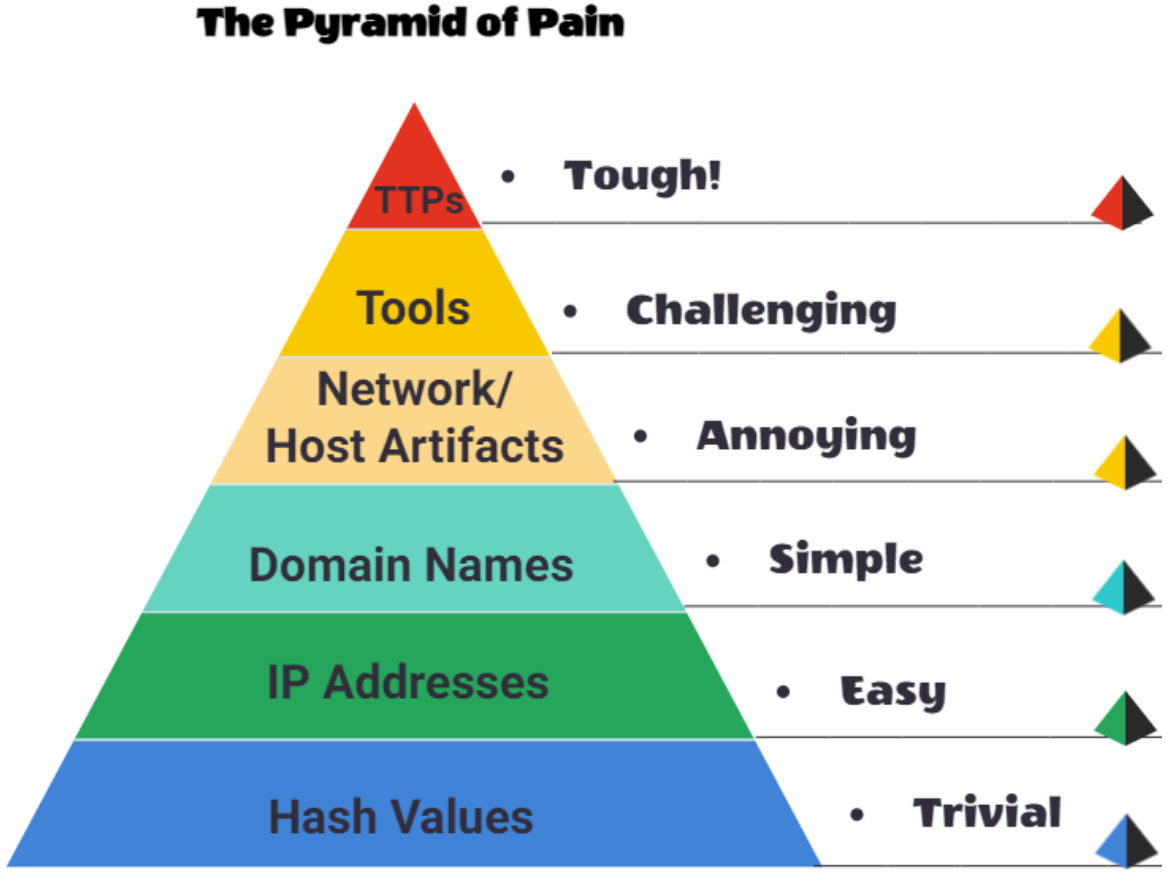
NTT DATA

IoCs Prioritization Criteria

TLP:CLEAR

Analysis of Our Security Environment（3/4）

- Firewall restricts traffic to ports 80 and 443, **blocking all other ports.**
- Prioritizing **domain-based IoCs over IP-based IoCs**, as they cause more disruption to attackers (Pyramid of Pain model).



Source: https://www.csnp.org/post/tryhackme-pyramid-of-pain-room

© 2024 NTT DATA Group Corporation

IoCs Prioritization Criteria

TLP:CLEAR

Analysis of Our Security Environment（4/4）

- In summary, the following four elements form the key requirements for IoC filtering:

1. Associated with advanced attackers
2. Related to C2 communications and data exfiltration
3. Limited to ports 80 and 443
4. Target domains instead of IP addresses

© 2024 NTT DATA Group Corporation

IoCs Prioritization Criteria

TLP:CLEAR

Analysis of Our Security Environment（4/4）

- In summary, the following four elements form the key requirements for IoC filtering:

1. **Associated with advanced attackers**
2. Related to C2 communications a
3. Limited to ports 80 and 443
4. Target Domains Instead of IP Ad

How to Identify IoCs associated with advanced attackers?

© 2024 NTT DATA Group Corporation

NTT DATA

IoCs Prioritization Criteria

TLP:AMBER+STRICT

How to Identify IoCs associated with advanced attackers?

Limited availability only at the conference venue

© 2024 NTT DATA Group Corporation

IoCs Prioritization Criteria

TLP:AMBER+STRICT

How to Identify IoCs associated with advanced attackers?

Limited availability only at the conference venue

© 2024 NTT DATA Group Corporation

IoCs Prioritization Criteria

TLP:AMBER+STRICT

Risk Score Calculation Logic By NTTDATA-CERT

Limited availability only at the conference venue

© 2024 NTT DATA Group Corporation

IoCs Prioritization Criteria

TLP:CLEAR

Risk Score Calculation Logic By NTTDATA-CERT

- Integrated the results of our data analysis with the requirement to prioritize C2-related IoCs to develop a risk score calculation logic.
- The IoC risk is evaluated using a four-level scoring system:

  - ✓ 0 – 30 points: Low
  - ✓ 40 – 60 points: Medium
  - ✓ 70 – 80 points: High
  - ✓ 90 – 100 points: Critical

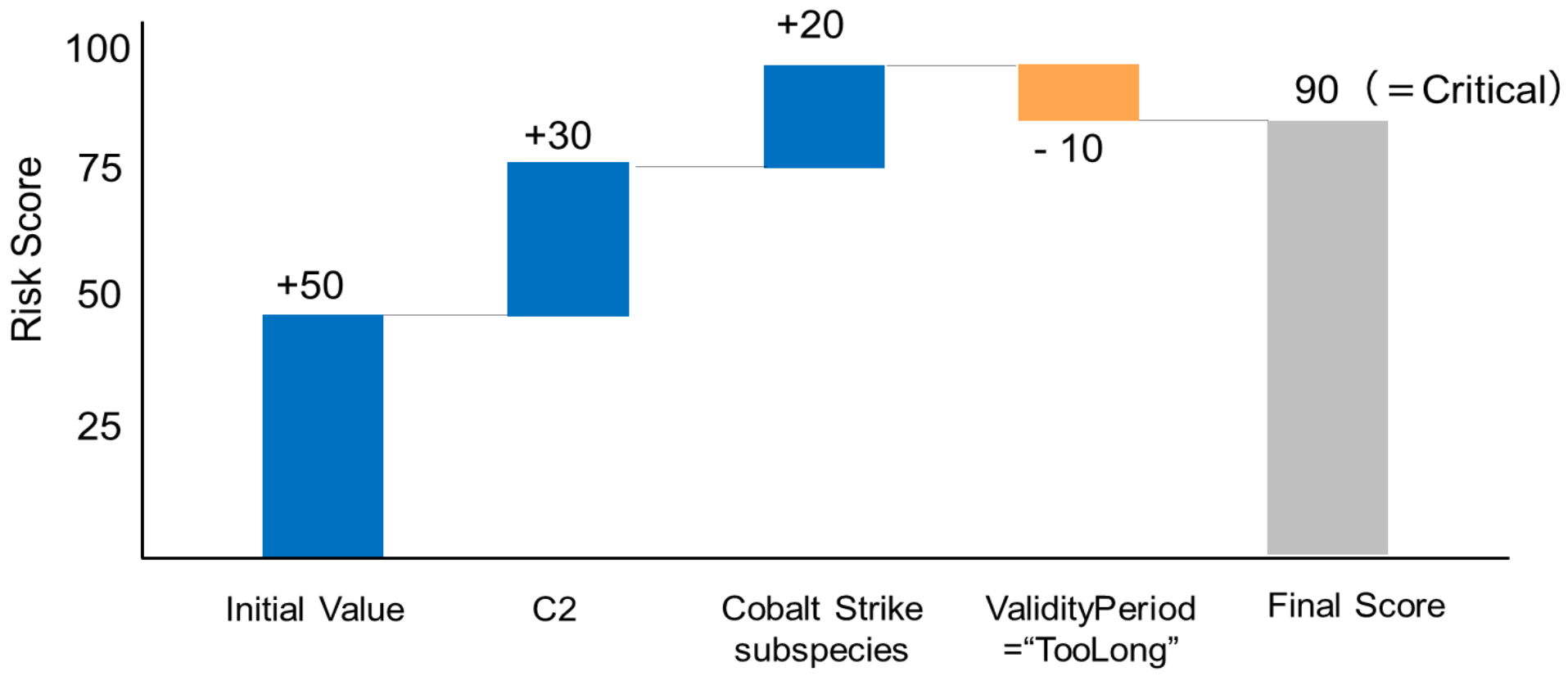
© 2024 NTT DATA Group Corporation

IoCs Prioritization Criteria

TLP:CLEAR

Risk Score Calculation Logic By NTTDATA-CERT

- Examples of "Critical" Risk Score is as follows:



© 2024 NTT DATA Group Corporation

NTT DATA

IoCs Prioritization Criteria

TLP:CLEAR

Real-World Example

- Identified ThreatFox as a **reliable information source with sufficient context.**
- **Registers around 500 IoCs daily, risking capacity overload of security devices.**
- **Manual verification of each IoC's impact on operations is impractical.**

Date (UTC)	IOC	Malware	Tags	Reporter
2025-01-06 06:56	103.15.186.10:443	Brute Ratel C4	as2519 BruteRatel c2 censys	skocherhan
2025-01-06 06:45	38.49.56.2:56004	AsyncRAT	asyncrat	abuse_ch
2025-01-06 06:45	38.49.56.2:56005	AsyncRAT	asyncrat	abuse_ch
2025-01-06 06:45	38.49.56.2:56003	AsyncRAT	asyncrat	abuse_ch
2025-01-06 06:35	185.194.236.52:443	DeimosC2	AS48314 c2 Deimos shodan	skocherhan

Source: ThreatFox | Browse IOCs

© 2024 NTT DATA Group Corporation

NTT DATA

IoCs Prioritization Criteria

TLP:CLEAR

Real-World Example

- Applied IoC Prioritization Criteria to IoC collected from ThreatFox.
- Filtering "High" and "Critical" risk IoCs reduced daily collection to ~80 IoCs.
- Further focusing on domain-based IoCs reduced it to ~50 IoCs per day.
- **Achieved a 90% reduction in collected IoCs**, prioritizing those most relevant to our environment.

No	Items	Total	Low	Medium	High	Critical
1	Total Count（5 Days）	1,420	459	548	398	15
2	After Applying Domain Filter	-	-	-	261	8
3	Daily Average (Rounded Up)	284	-	-	**52**	**2**

※ Port-Based Filtering Already Applied

© 2024 NTT DATA Group Corporation

NTT DATA

IoCs Lifecycle Model

© 2024 NTT DATA Group Corporation

IoCs Lifecycle Model

TLP:CLEAR

Investigation and Interview Findings For IoCs Lifecycle Model

- Investigated essential information for building an IoC lifecycle model.
- Conducted interviews to **identify reasons for retaining outdated IoCs in operations.**
- Key findings from the investigation and interview are summarized below.

No	Items	Findings	Necessary information
1	Investigation	Research focused on past FIRST Conference presentations, with **limited information on IoC lifecycle management.**	IoCs Lifecycle Characteristics in Our Environment
2	Interview	Found some organizations remove IoCs on fixed cycles (e.g., 3 or 6 months) **without clear justification.**	
3		SOC team raised concerns about IoC removal, **fearing it may result in missed threats**, causing hesitation to adopt removal processes.	Data-Driven Removal Criteria

© 2024 NTT DATA Group Corporation

NTT DATA

IoCs Lifecycle Model

Data-Driven Removal Criteria

TLP:AMBER+STRICT

Limited availability only at the conference venue

© 2024 NTT DATA Group Corporation

IoCs Lifecycle Model

TLP:CLEAR

Agreement on Lifecycle Model Operations with Stakeholders

- Consulted with SOC team and internal experts on implementing the Lifecycle Model.
- **Approved for operational use after confirming that IoC removal risks were sufficiently mitigated.**
- Lifecycle Model expected to be fully operational by the end of FY2024.

© 2024 NTT DATA Group Corporation

NTT DATA

Conclusion

© 2024 NTT DATA Group Corporation

Conclusion

TLP:CLEAR

- Developed the **IoCs Prioritization Criteria** and **Lifecycle Model** to tackle two common challenges:

1. IoC registration limits on security devices pose a significant challenge, as failing to filter out low-risk or outdated IoCs can **prevent the timely registration of high-risk, emerging threats, leaving critical gaps in defense（IoC Capacity Constraints）**

2. Retaining outdated IoCs increases false positives, **leading to alert fatigue and operational inefficiencies in SOC teams（False Positive Fatigue）**

- Ensured **prioritization of high-risk, relevant IoCs while systematically removing outdated, low-risk ones to mitigate capacity issues and alert fatigue.**

© 2024 NTT DATA Group Corporation

NTT DATA