



The background of the slide features a photograph of a lighthouse on a rocky cliff at sunset. The sky is a gradient from blue to orange and yellow. The lighthouse is illuminated, casting a warm glow. In the foreground, there's some dark, silhouetted vegetation.

**DEBUG CONSULTING**

**MISP** 

# Threat Sharing

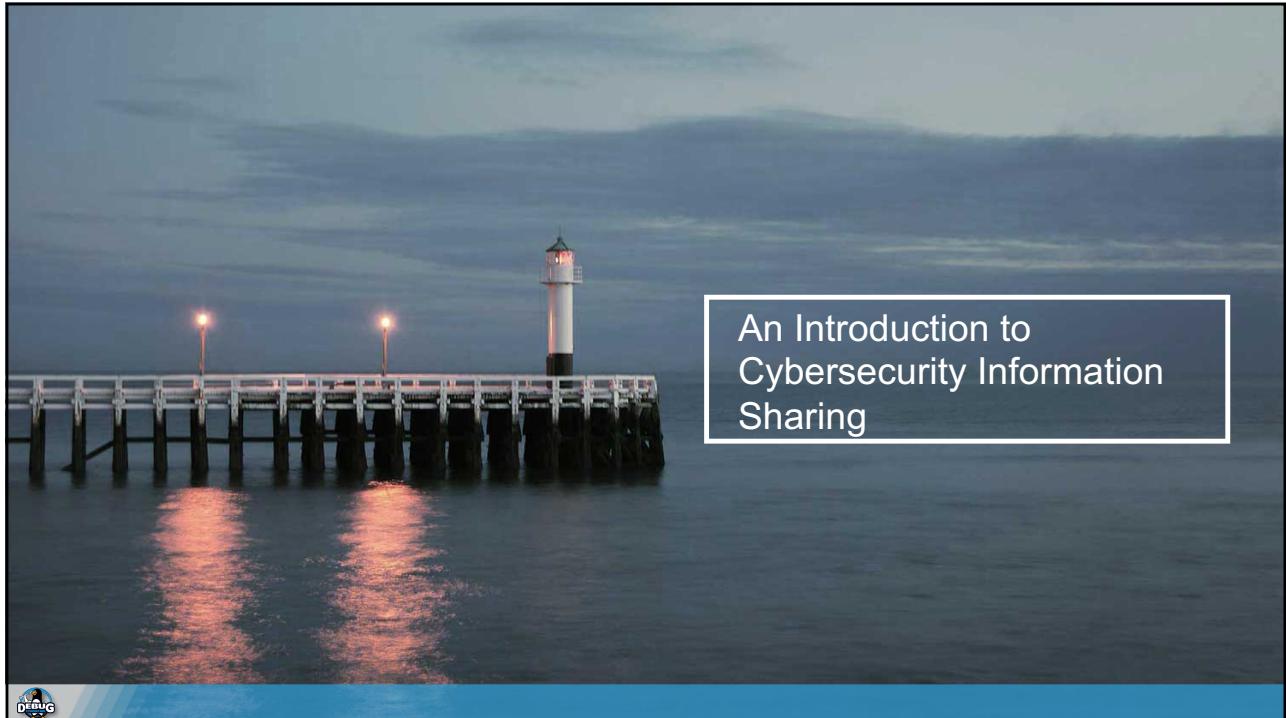
Malware Information Sharing Platform and  
Migration solutions for  
**Office of Insurance Commission (OIC)**



The background of the slide features a photograph of a wooden pier extending into a body of water at dusk or night. A single street lamp on the pier is illuminated, casting light onto the wet wooden planks and the surrounding water. The overall atmosphere is calm and slightly mysterious.

## Agenda

- 01** Introduction to Cybersecurity Information Sharing
- 02** General usage of MISP
- 03** Administration of MISP 2.4



## MISP's Begins

- ในกลุ่มคณะทำงานการวิเคราะห์มัลแวร์ในปี 2555 พากเข้าพบว่ามีทำงานเกี่ยวกับการวิเคราะห์มัลแวร์ตัวเดียวกัน
- มีความต้องการแบ่งปันข้อมูลด้วยวิธีที่ง่ายและเป็นอัตโนมัติเพื่อหลีกเลี่ยงไม่ให้งานซ้ำซ้อน
- Christophe Vandeplas นำเสนองานของเขางานแพลตฟอร์ม ซึ่งที่ต่อมาภายเป็น MISP
- MALWG ใช้แพลตฟอร์ม MISP เวอร์ชันแรก และขอเสนอแนะที่เพิ่มขึ้นของผู้ใช้ช่วยให้เราสร้างแพลตฟอร์มที่ได้รับการปรับปรุง
- MISP เป็นการพัฒนาที่ขับเคลื่อนโดยชุมชน



## CIRCL

Computer Incident Response Center Luxembourg (CIRCL) เป็นโครงการริเริ่มที่ขึ้บเคลื่อนโดยรัฐบาล ซึ่งตั้งขึ้นมาเพื่อดำเนินงานการตอบสนองต่อภัยคุกคามและเหตุการณ์ด้านความปลอดภัยของคอมพิวเตอร์อย่างเป็นระบบ

CIRCL คือ CERT สำหรับภาคเอกชน ประจำกม และหน่วยงานนอกรัฐในลักเซมเบิร์ก และดำเนินการโดย securitymadein.lu



## MISP and CIRCL

- CIRCL ได้รับคำสั่งจากกระทรวงเศรษฐกิจและพาณิชย์ที่เป็น CERT แห่งชาติลักเซมเบิร์กสำหรับภาคเอกชน
- CIRCL เป็นผู้นำในการพัฒนาแพลตฟอร์มข่าวกรองภัยคุกคามแบบโอเพ่นซอร์ส MISP ซึ่งใช้งานโดยชุมชนทางการทหารหรือหน่วยข่าวกรอง บริษัทเอกชน ภาครัฐ เน็ตเวิร์ก ระดับประเทศ และ LEA ทั่วโลก
- CIRCL ขับเคลื่อนชุมชน MISP ขนาดใหญ่หลายแห่งที่แบ่งปันข้อมูลภัยคุกคาม-ข่าวกรองรายวัน



## MISP?

- MISP เป็นแพลตฟอร์มแบ่งปันข้อมูลภัยคุกคามที่เป็นซอฟต์แวร์โอเพ่นซอร์ส
- เครื่องมือที่รวบรวมข้อมูลจากพันธมิตร นักวิเคราะห์ เครื่องมือ และ ฟีด
- ทำให้เป็นบรรทัดฐาน หาความสัมพันธ์ เสริมสร้างข้อมูล
- ช่วยให้ทีม และชุมชนทำงานร่วมกันได้
- ป้อนข้อมูลให้เครื่องมือป้องกันอัตโนมัติ และเครื่องมือวิเคราะห์



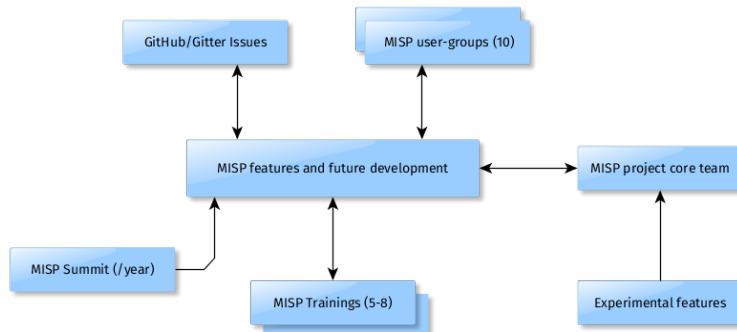
## พัฒนาขึ้นจากข้อคิดเห็นของผู้ใช้งาน

มีผู้ใช้แพลตฟอร์มแบ่งปันข้อมูลหลายประเทศ เช่น MISP:

- นักวิเคราะห์มัลแวร์ ต้องการแบ่งปันตัวบ่งชี้การวิเคราะห์กับเพื่อนร่วมงานที่เกี่ยวข้อง
- นักวิเคราะห์ความปลอดภัย ค้นหา ตรวจสอบ และการใช้ตัวบ่งชี้ในการรักษาความปลอดภัย
- นักวิเคราะห์ข่าวกรอง รวบรวมข้อมูลเกี่ยวกับกลุ่มผู้โจมตี
- ผู้บังคับใช้กฎหมาย อ้างอิงกับตัวบ่งชี้เพื่อสนับสนุนหรือ ข้อมูลเบาะแสในกรณีทำ DFIR
- ทีมวิเคราะห์ความเสี่ยง ต้องการทราบเกี่ยวกับภัยคุกคามใหม่ แนวโน้มและเหตุการณ์ที่เกิดขึ้น
- นักวิเคราะห์การอํอโคง ต้องการแบ่งปันตัวชี้วัดการซ่อโคงทางการเงิน เพื่อตรวจสอบการอํอโคง



## โครงสร้างการทำงานร่วมกัน



## วัตถุประสงค์การใช้งานจากกลุ่มผู้ใช้

- แบ่งปันตัวบ่งชี้สำหรับเรื่องการตรวจจับ
  - มีระบบที่ติดไวรัสในโครงสร้างพื้นฐาน หรือที่กำลังใช้งานอยู่หรือไม่?
- แบ่งปันตัวบ่งชี้การเพื่อทำการบล็อก
  - นำใช้คุณลักษณะมาใช้เพื่อบล็อก หลอกล่อ หรือเปลี่ยนเส้นทาง
- แบ่งปันตัวบ่งชี้เพื่อดำเนินการทางกฎหมาย
  - รวบรวมข้อมูลเกี่ยวกับขบวนการการโจมตี มีความเกี่ยวข้องกันหรือไม่? ใครกำลังแทรกเป็นเป้าหมาย? ใครคือผู้โจมตี?
- ข้อมูลขัดแย้งต่าง ๆ (เช่น ผลบวกเท่าที่มีผลกระทบต่างไป)

## กลุ่มผู้ใช้งาน MISP

- กลุ่มที่มีการแบ่งปันข้อมูลด้วยวัตถุประสงค์เฉพาะ
- CIRCL ที่ดำเนินงานดูแล MISP จำนวนมาก (มากกว่า 1,200 องค์กร ที่มีผู้ใช้มากกว่า 4,000 คน)
- กลุ่มที่เชื่อมโยงกันระหว่างกลุ่มอุตสาหกรรม
- ภาคการเงิน (ธนาคาร, ISACs, องค์กรรับชำระเงิน) ใช้ MISP เป็นขั้นตอนในการแลกเปลี่ยนข่าวสาร
- หน่วยงานทหารหรือหน่วยงานระหว่างประเทศ (NATO, Military CSIRTs, n/g CERT and etc.)
- ผู้ให้บริการด้านความปลอดภัย ที่ก่อตั้งกลุ่มเข้าร่วมกัน หรือเชื่อมต่อกับกลุ่มผู้ใช้งาน
- ชุมชนเฉพาะที่จัดตั้งขึ้นเพื่อจัดการกับปัญหาเฉพาะกิจ (COVID-19 MISP)

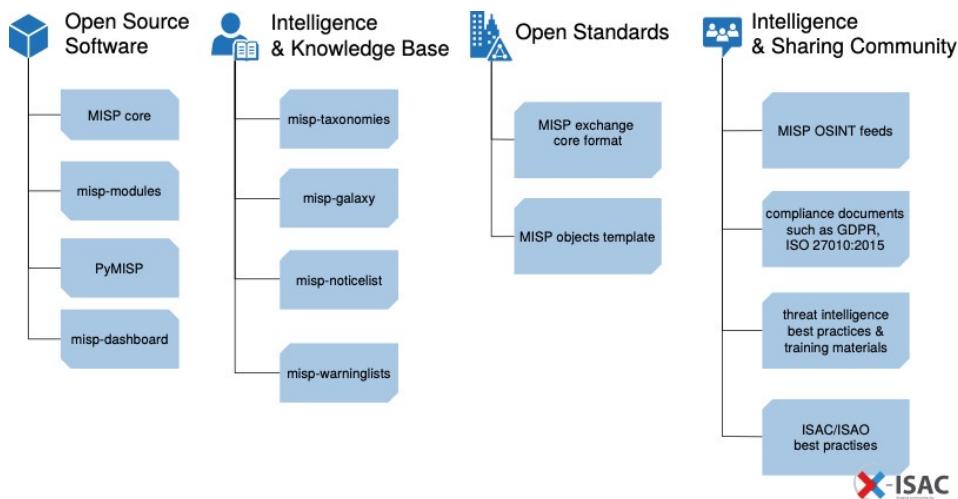


## ความท้าทายในการแบ่งปันข่าวสาร

- ความยากลำบากในการแบ่งปันไม่ใช่ปัญหาทางเทคนิค แต่มักเป็นเรื่องของสังคมหรือธุรกิจ ( เช่น ความไว้วางใจ )
- ข้อกำหนดทางกฎหมาย
  - ครอบกฎหมาย ไม่อนุญาตให้แบ่งปันข้อมูล
  - ความเสี่ยงจากการรั่วไหลของข้อมูลสูงเกินไป และเสี่ยงเกินไปสำหรับองค์กรหรือพันธมิตร
- ข้อจำกัดในทางปฏิบัติ
  - ไม่มีข้อมูลที่จะแบ่งปัน
  - ไม่มีเวลาประมวลผลหรือมีส่วนร่วมกับตัวชี้วัด
  - แบบจำลองการจัดประเภทมีความไม่เข้ากัน
  - เครื่องมือสำหรับการแบ่งปันข้อมูลมีการเชื่อมโยงเป็นรูปแบบเฉพาะ หรือใช้รูปแบบที่แตกต่างกัน



## โครงสร้างทั้งไปของ MISP



## คัพท์ที่เกี่ยวข้อง

- ระดับข้อมูล
  - Events เป็นตัวเก็บข้อมูลที่เริ่มโยงได้ตามบริบทต่าง ๆ
  - Attributes ข้อมูลจำเพาะ ซึ่งสามารถเป็นตัวบ่งชี้ (Indicator) หรือข้อมูลสนับสนุนได้
  - Objects เป็นต้นแบบที่กำหนดขึ้น เพื่อให้มีองค์ประกอบของ Attribute
  - Object references เป็นตัวเชื่อมอ้างอิงกับกลุ่มต้นแบบอื่น ๆ
  - Sighting เป็นตัวบ่งบอกเวลาที่เกิดเหตุการณ์ตามตัวกำหนดที่ตรวจสอบ
- ระดับบริบท
  - Tags เป็นป้ายกำกับที่ติดมากับเหตุการณ์/คุณลักษณะและสามารถมาจากอนุกรมวิธาน\* (Taxonomies) ได้
  - Galaxy-clusters เป็นรายการฐานความรู้ที่ใช้ติดป้ายเหตุการณ์/แอ็ตทริบิวต์และมาจากการแลกเปลี่ยน\*\*
  - Cluster relationships แสดงถึงความสัมพันธ์ที่กำหนดให้ล่วงหน้าระหว่างคลัสเตอร์

\* การจัดหมวดหมู่, การก่อเกตเวย์ของหมวดหมู่

## คำศัพท์เกี่ยวกับตัวชี้วัด

- Indicators<sup>1</sup>

- ตัวบ่งชี้มีรูปแบบที่สามารถใช้เพื่อตรวจจับกิจกรรมทางไซเบอร์ที่น่าสงสัยหรือเป็นอันตราย

- Attributes

ใน MISP สามารถเป็นตัวบ่งชี้เครือข่าย (เช่นที่อยู่ IP) ตัวบ่งชี้ระบบ (เช่นสตริงในหน่วยความจำ) หรือแม้แต่รายละเอียดบัญชีธนาคาร

- ประเภท (เช่น MD5, url) คือวิธีการอธิบายแอ็ตทริบิวต์

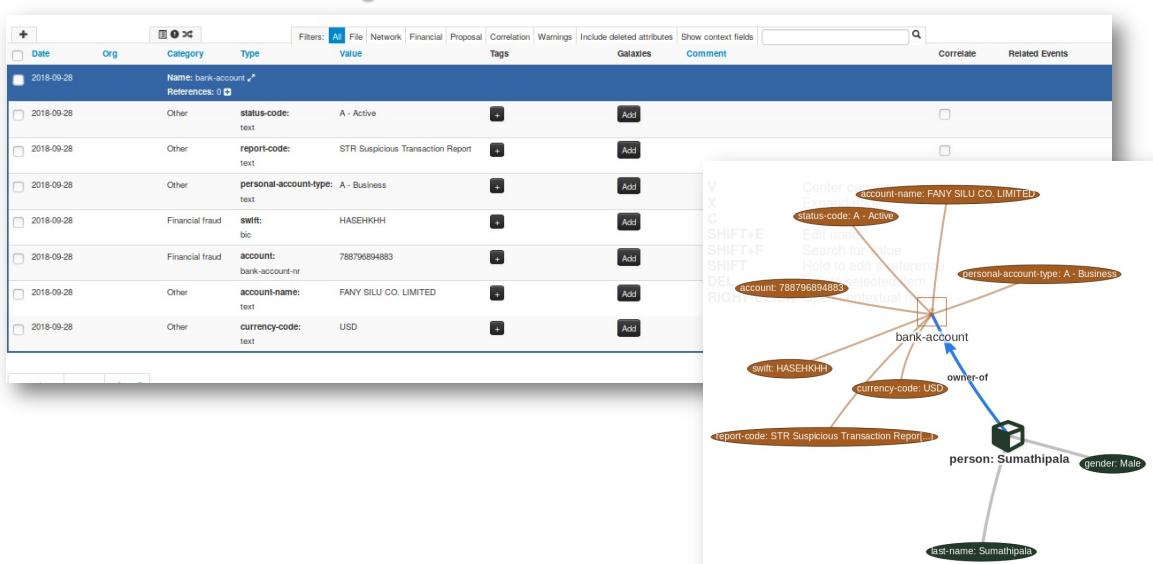
➤ แอ็ตทริบิวต์จะอยู่ในหมวดหมู่เดียวกัน (เช่น Payload delivery) ซึ่งใส่ไว้ในบริบท (Context)

- IDS flag บนแหล่งทรัพยากร์ที่อยู่ให้ระบุได้ว่าแหล่งทรัพยากร์สามารถใช้สำหรับการตรวจสอบได้โดยอัตโนมัติหรือไม่

<sup>1</sup>IoC (ลักษณะของการติดค่าอง) เป็นร้านค้าของลักษณะ

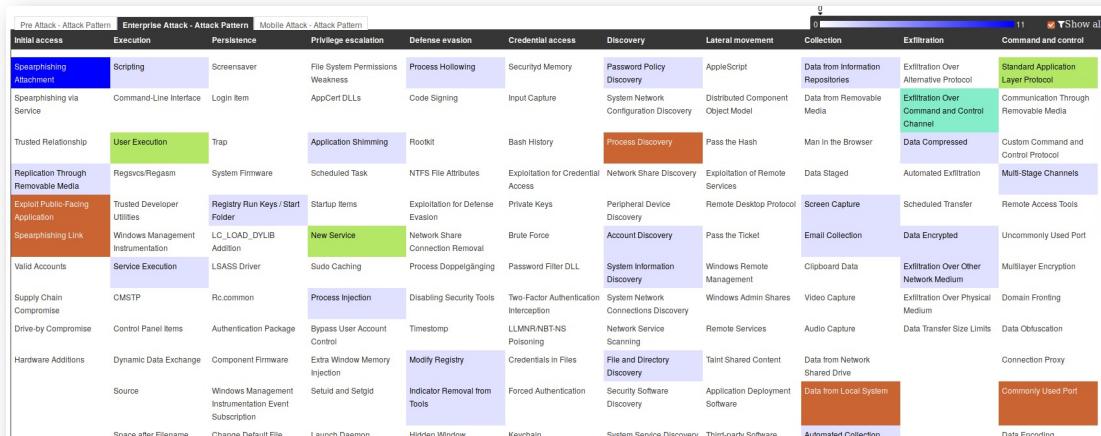


## ตัวอย่าง : โมเดลข้อมูล



## บริบทและการจับกลุ่มข้อมูล

- MISP ทำงานร่วมกันในระดับ Event และระดับแอ็ตทริบิวต์ MITRE's Adversarial Tactics, Techniques และ Common Knowledge (ATT&CK)



The screenshot shows the MITRE ATT&CK matrix, which is a grid of tactics and techniques. The columns represent platforms: Pre Attack - Attack Pattern, Enterprise Attack - Attack Pattern, and Mobile Attack - Attack Pattern. The rows represent tactics. Each cell contains a technique name and its corresponding ATT&CK ID. The matrix is color-coded by tactic category.

	Pre Attack - Attack Pattern	Enterprise Attack - Attack Pattern	Mobile Attack - Attack Pattern							
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Exfiltration	Command and control
Spearphishing Attachment	Scripting	Screensaver	File System Permissions Weakness	Process Hollowing	Securid Memory	Password Policy Discovery	AppleScript	Data from Information Repositories	Exfiltration Over Alternative Protocol	Standard Application Layer Protocol
Spearphishing via Service	Command-Line Interface	Login Item	ApoCert DLLs	Code Signing	Input Capture	System Network Configuration Discovery	Distributed Component Object Model	Data from Removable Media	Exfiltration Over Command and Control Channel	Communication Through Removable Media
Trusted Relationship	User Execution	Trap	Application Shimming	Rootkit	Bash History	Process Discovery	Pass the Hash	Man in the Browser	Data Compressed	Custom Command and Control Protocol
Replication Through Removable Media	Regsvcs/Regasm	System Firmware	Scheduled Task	NTFS File Attributes	Exploitation for Credential Access	Network Share Discovery	Exploitation of Remote Services	Data Staged	Automated Exfiltration	Multi-Stage Channels
Exploit Public-Facing Application	Trusted Developer Utilities	Registry Run Keys / Start Folder	Startup Items	Exploitation for Defense Evasion	Private Keys	Peripheral Device Discovery	Remote Desktop Protocol	Screen Capture	Scheduled Transfer	Remote Access Tools
Spearphishing Link	Windows Management Instrumentation	LC_LOAD_DYLIB Addition	New Service	Network Share Connection Removal	Brute Force	Account Discovery	Pass the Ticket	Email Collection	Data Encrypted	Uncommonly Used Port
Valid Accounts	Service Execution	LSASS Driver	Sudo Caching	Process Doppelgänging	Password Filter DLL	System Information Discovery	Windows Remote Management	Clipboard Data	Exfiltration Over Other Network Medium	Multi-layer Encryption
Supply Chain Compromise	CMSTP	Rc-common	Process Injection	Disabling Security Tool	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Video Capture	Exfiltration Over Physical Medium	Domain Fronting
Drive-by Compromise	Control Panel Items	Authentication Package	Bypass User Account Control	Timestamp	LLMNR/NBT-NS Poisoning	Network Service Scanning	Remote Services	Audio Capture	Data Transfer Size Limits	Data Obfuscation
Hardware Additions	Dynamic Data Exchange	Component Firmware	Extra Window Memory Injection	Modify Registry	Credentials in Files	File and Directory Discovery	Taint Shared Content	Data from Network Shared Drive		Connection Proxy
Source	Windows Management Instrumentation Event Subscription	Seuid and Setgid	Indicator Removal from Tools	Forced Authentication	Security Software Discovery	Application Deployment Software		Data from Local System		Commonly Used Port
Space after Filename	Change Default File	Launch Daemon	Hidden Window	Keychain	System Service Discovery	Third-party Software	Automated Collection			Data Encoding



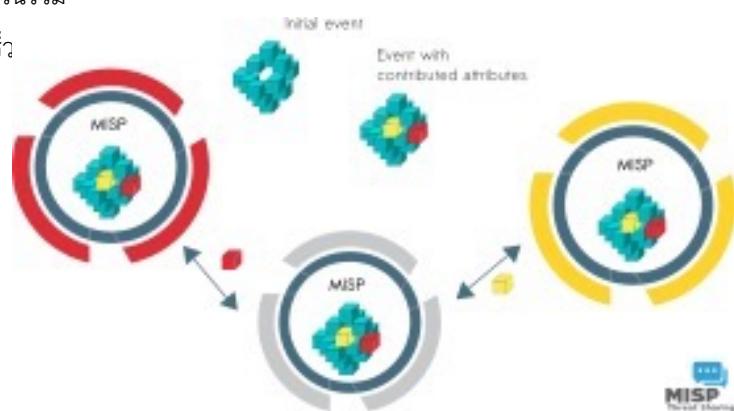
## การแบ่งปัน

- การแชร์ผ่านรายชื่อการแจกราย - กลุ่มการแบ่งปัน (Sharing groups)
- ตัวแทน (Delegation) สำหรับการแบ่งปันข้อมูลโดยไม่ระบุตัวตน
- ข้อเสนอ (Proposal) และเหตุการณ์เพิ่มเติม (Extended events) สำหรับการแบ่งปันข้อมูลร่วมกัน
- การซิงโครไนซ์ ระบบฟิด, การแบ่งปันแบบ off-line (air-gapped)
- ผู้ใช้กำหนด ตัวกรองการแบ่งปัน สำหรับวิธีการตั้งกล่าวข้างต้นทั้งหมด
- การแก้ไขข้อมูล ข้ามอินสแตนซ์สำหรับการค้นหาชุดข้อมูลขนาดใหญ่อย่างรวดเร็ว
- รองรับ multi-MISP สำหรับภัยใน (เครือข่าย)



## MISP core กระจายฟังก์ชันการทำงานร่วมกัน

- ฟังก์ชันหลักของ MISP คือการแชร์ในที่ที่ทุกคนสามารถเป็นผู้รับข้อมูลและ/หรือผู้ร่วมให้ข้อมูล/ผู้สร้างข้อมูลได้
- เข้าถึงได้อย่างรวดเร็วโดยไม่ต้องมีส่วนร่วม
- เข้าถึงง่าย คุ้นเคยกับระบบได้รวดเร็ว



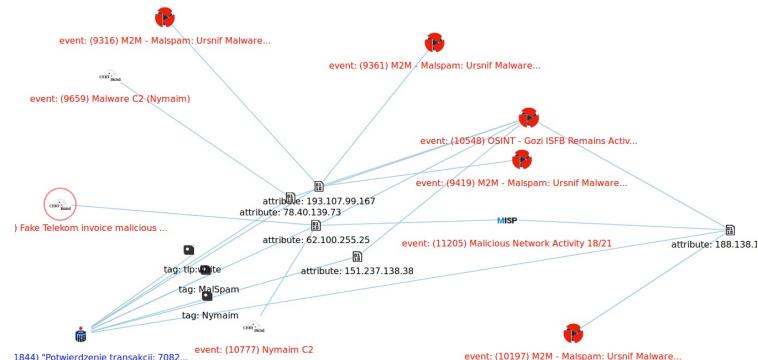
## การจัดการคุณภาพข้อมูล

- การหาความสัมพันธ์ของข้อมูล (Correlating data)
- กระบวนการตอบกลับ (feedback) จากการตรวจจับผ่าน Sightings
- การจัดการผลบวกเท็จ (False-positive) ผ่านระบบรายการเตือน
- ระบบเพิ่มความสมบูรณ์ของข้อมูล (Enrichment) ผ่าน MISP-modules
- การทำงานร่วมกัน (Integrations) กับเครื่องมือและรูปแบบต่างๆ มากมาย
- API ที่ยืดหยุ่นและรองรับไลบรารี เช่น PyMISP เพื่อให้การทำงานร่วมกันง่ายขึ้น
- ไทม์ไลน์และการให้ข้อมูลเป็นบริบทชั่วคราว
- ห่วงโซ่เต็มรูปแบบสำหรับการจัดการวงจรชีวิตตัวบ่งชี้ (indicator life-cycle management)



## คุณสมบัติความสัมพันธ์ : เครื่องมือสำหรับนักวิเคราะห์

เพื่อยืนยันการค้นพบ (เช่น นี่เป็นแคมเปญเดียวกันหรือไม่) เสริมการวิเคราะห์ (เช่น นักวิเคราะห์คนอื่นๆ มีสมมติฐานเหมือนกันหรือไม่) ยืนยันลักษณะเฉพาะ (เช่น ที่อยู่ IP ที่ได้จากการตักกิใช้สำหรับแคมเปญเดียวกันหรือไม่) หรือคาดคะเนว่า ภัยคุกคามนี้เป็นของใหม่หรือไม่โดยเจอบอกกลุ่มของคุณ



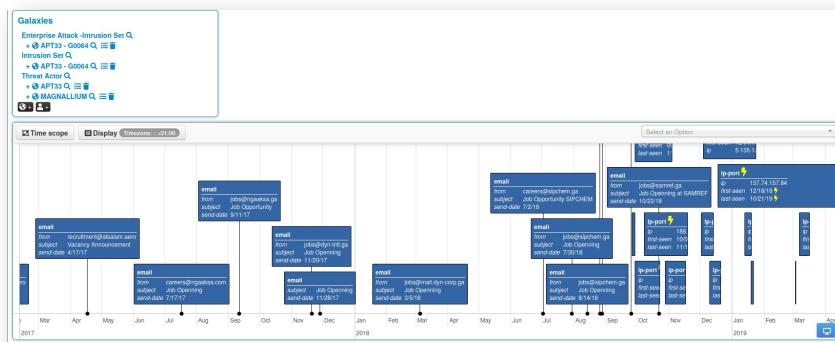
## รองรับ Sightings

- เราหรือกลุ่มได้พบ/เคยพบ ตามชุดข้อมูลดังกล่าวมาก่อนหรือไม่
- นอกจากนี้ ระบบ sighting ยังรองรับการตรวจสอบเชิงลบ (FP) และ sighting หมวดอาชญากรรม
- sighting สามารถทำได้ผ่าน API หรือ UI
- หลายกรณี การให้คะแนนตัวบ่งชี้ (scoring indicators) สามารถพิจารณาได้จาก sighting จากผู้ใช้
- สำหรับข้อมูลปริมาณมาก สามารถใช้ SightingDB โดย Devo



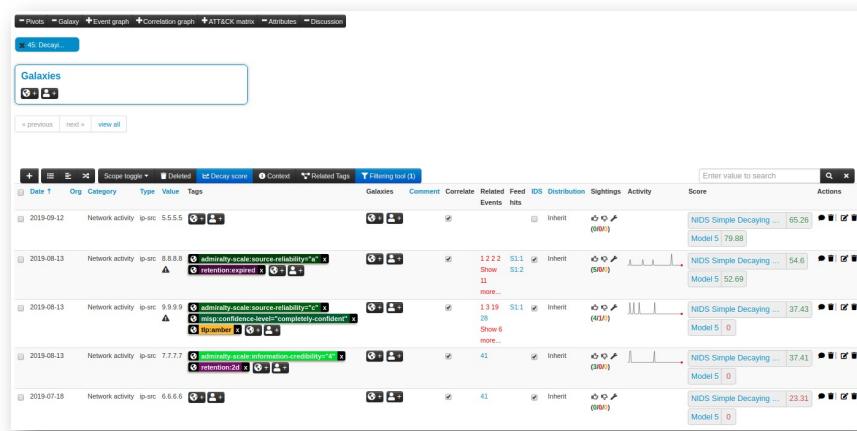
## ไทร์ไลน์และการให้ข้อมูลเป็นบริบททั่วไป

- จุดข้อมูล ที่พบรัตัวครั้งแรกและครั้งล่าสุด
- จุดข้อมูลทั้งหมดแสดงตามช่วงเวลา
- เปิดใช้งานการแสดงภาพและการปรับกรอบเวลาตัวปั่นชี้



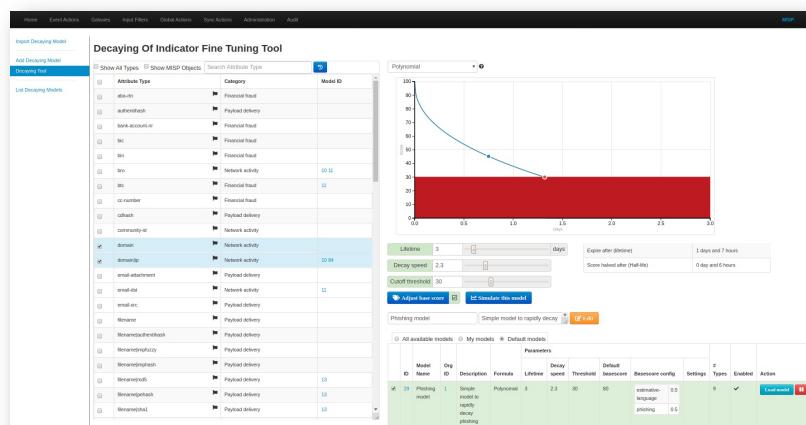
## การบริหารงจตัวชี้วัด จากการเลื่อมของตัวชี้วัด

- ปุ่มเปิด/ปิดคะแนน (Decay score toggle button)
  - แสดงคะแนนสำหรับแต่ละโมเดล (Model) ที่เกี่ยวข้องกับประเภทแอ็ตทริบิวต์ (Attribute type)



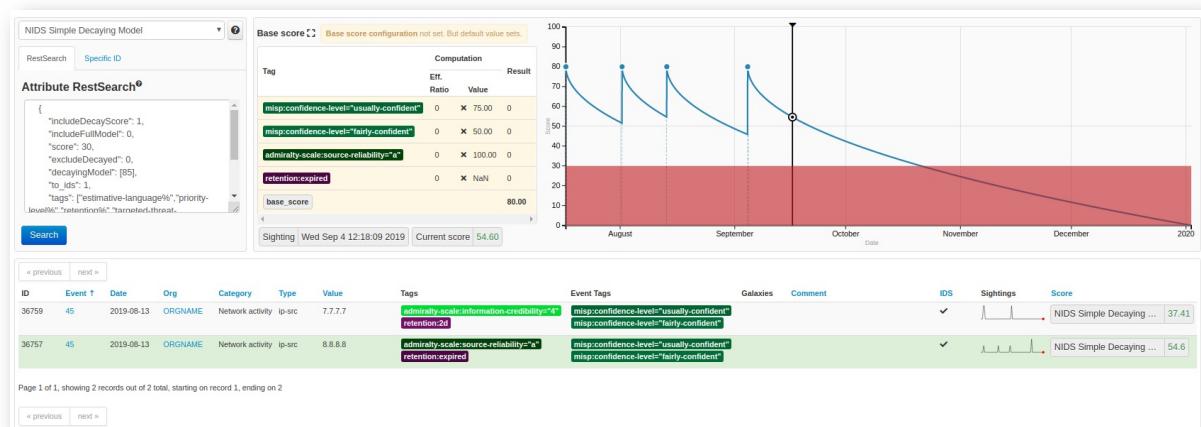
## การเลื่อนของตัวบ่งชี้: เครื่องมือปรับแต่งอย่างละเอียด

- สร้างแก้ไข แสดงภาพ ทำการแมป



## การเลื่อนของตัวบ่งชี้ : เครื่องมือจำลอง

- จำลองแอ็คทริบิวต์ด้วยแบบจำลองที่แตกต่างกัน



## เริ่มต้นด้วย “ข้อมูล”

- เริ่มต้นด้วยไฟด์จาก CIRCL OSINT (เลือกมาจากการที่ต้องการจะใช้ใน MISP) ใน MISP เพื่อให้ผู้ใช้ลดความยุ่งยากในการเริ่มต้น
- รูปแบบของไฟด์ OSINT ขึ้นอยู่กับมาตรฐาน MISP JSON ที่ได้มาจากเซิร์ฟเวอร์ TLS/HTTP ระยะไกล
- ผู้ให้บริการเนื้อหาอื่น ๆ สามารถจัดเตรียมไฟด์ MISP ของตนเองได้
- อนุญาตให้ผู้ใช้ทดสอบการติดตั้ง MISP และการซิงโครไนซ์กับชุดข้อมูลจริง
- เปิดการสนับสนุนไฟด์ ข่าวกรองภัยคุกคามอื่น ๆ แต่ยังช่วยให้วิเคราะห์ข้อมูลที่ทับซ้อนกันได้<sup>1</sup>

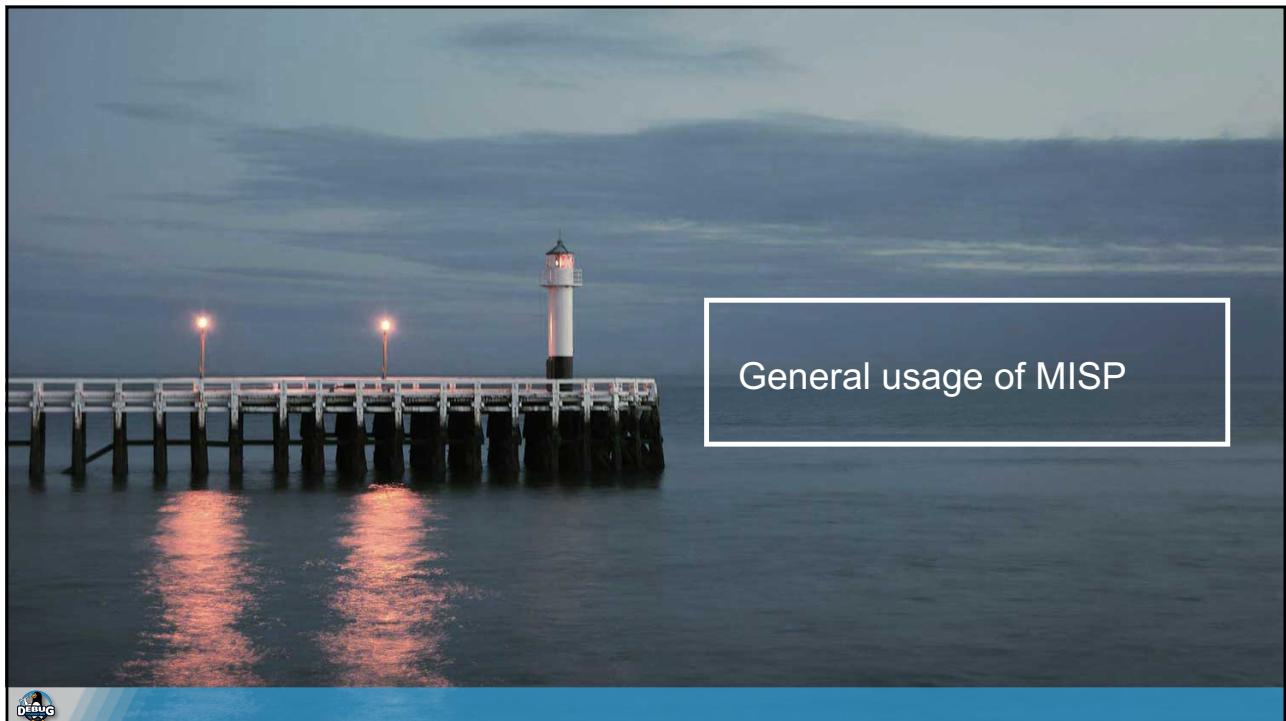
<sup>1</sup> ความที่หากเพิ่มขึ้นมาในกระบวนการเปลี่ยนข้อมูล



## บทสรุป

- แนวทางปฏิบัติในการแบ่งปันข้อมูลมาจากการผู้ใช้งานและตัวอย่าง (เช่น การเรียนรู้โดยการเลียนแบบจากข้อมูลที่แบ่งปัน)
- MISP เป็นเพียงเครื่องมือ สิ่งที่สำคัญคือแนวทางปฏิบัติในการแบ่งปันขององค์กร เครื่องมือควรมีความโปร่งใสมากที่สุดเพื่อสนับสนุนผู้ใช้งาน
- ให้ผู้ใช้ปรับแต่ง MISP เพื่อให้สอดคล้องกับกรณีการใช้งานของกลุ่ม
- โครงการ MISP เกิดขึ้นจากการรวมกันของ ซอฟต์แวร์โอเพ่นซอร์ส มาตรฐานแบบเปิด แนวทางปฏิบัติที่ดี และกลุ่มคนเพื่อทำให้การแบ่งปันข้อมูล มีการทำงานใกล้ความเป็นจริงที่สุด





## การเข้าใช้งาน



## MISP - การใช้งานทั่วไป

- Data model
- Viewing data
- Creating data
- Co-operation
- Distribution
- Exports

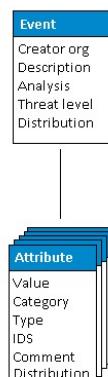


## MISP - Event (MISP's basic building block)

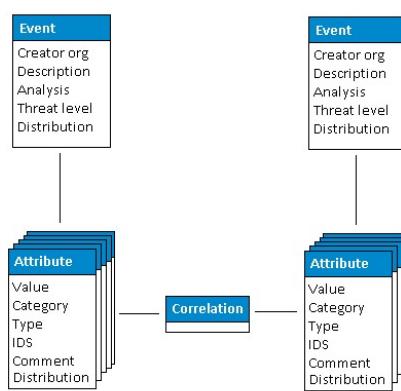
Event
Creator org
Description
Analysis
Threat level
Distribution



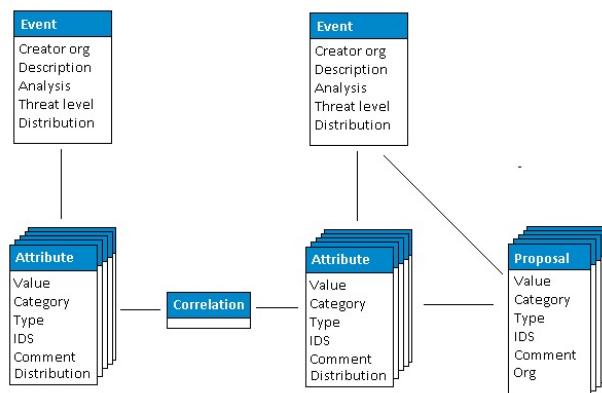
## MISP - Event (Attributes, giving meaning to events)



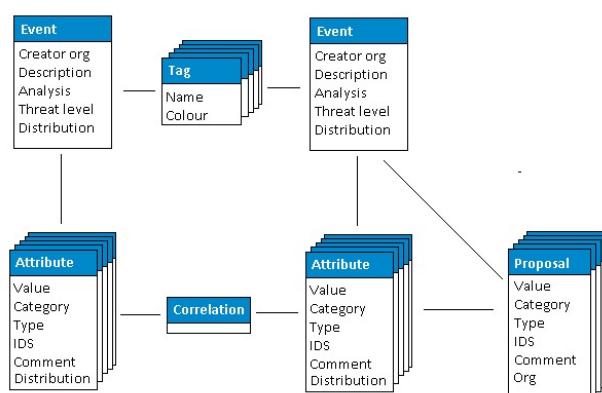
## MISP - Event (Correlations on similar attributes)



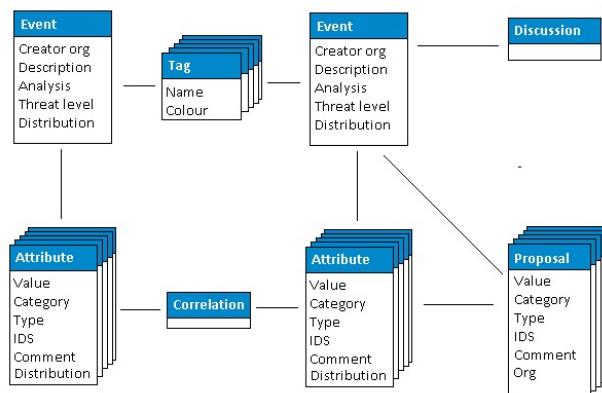
## MISP - Event (Proposals)



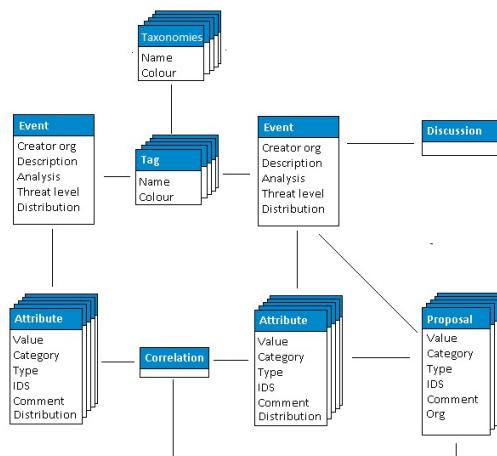
## MISP - Event (Tags)



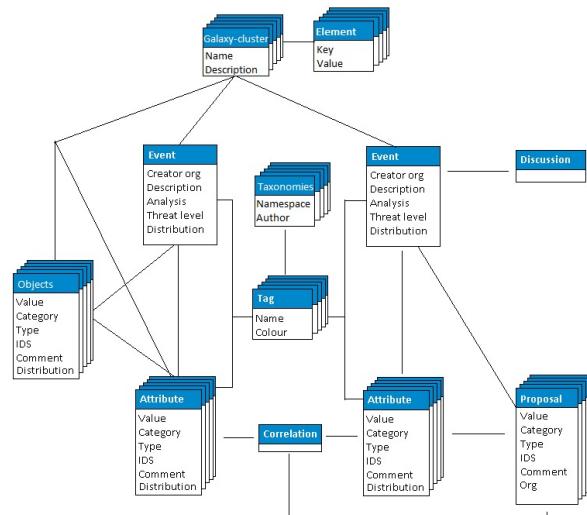
## MISP - Event (Discussions)



## MISP - Event (Taxonomies and proposal correlations)



## MISP - Event (The state of art MISP Data model)



## MISP - Viewing the Event Index

- Event Index
  - Event context
  - Tags
  - Distribution
  - Correlations
- Filters

## MISP - Viewing an Event

- Event View
  - Event context
  - Attributes
    - Category/type, IDS, Correlations
  - Objects
  - Galaxies
  - Proposals
  - Discussions
- Tools to find what you are looking for
- Correlation graphs



## MISP - Creating and populating events in various ways

- The main tools to populate an event
  - Adding attributes / batch add
  - Adding objects and how the object templates work
  - Freetext import
  - Import
  - Templates
  - Adding attachments / screenshots
  - API



## MISP - Various features while adding data

- What happens automatically when adding data?
  - Automatic correlation
  - Input modification via validation and filters (regex)
  - Tagging / Galaxy Clusters
- Various ways to publish data
  - Publish with/without e-mail
  - Publishing via the API
  - Delegation



## MISP - Using the data

- Correlation graphs
- Downloading the data in various formats
- API (explained later)
- Collaborating with users (proposals, discussions, emails)



## MISP - Sync explained (if no admin training)

- Sync connections
- Pull/push model
- Previewing instances
- Filtering the sync
- Connection test tool
- Cherry pick mode



## MISP - Feeds explained (if no admin training)

- Feed types (MISP, Freetext, CSV)
- Adding/editing feeds
- Previewing feeds
- Local vs Network feeds

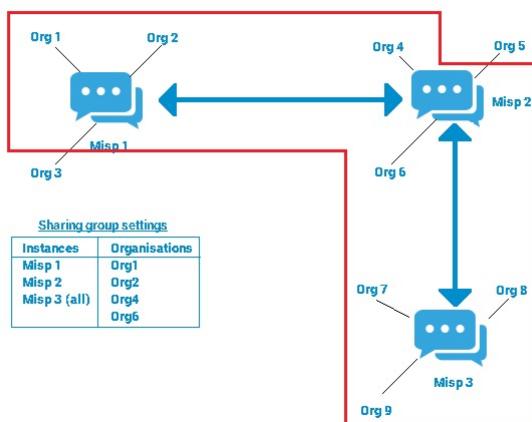


## MISP - Distributions explained

- Your Organisation Only
- This Community Only
- Connected Communities
- All Communities
- Sharing Group



## MISP - Distribution and Topology



## MISP - Exports and API

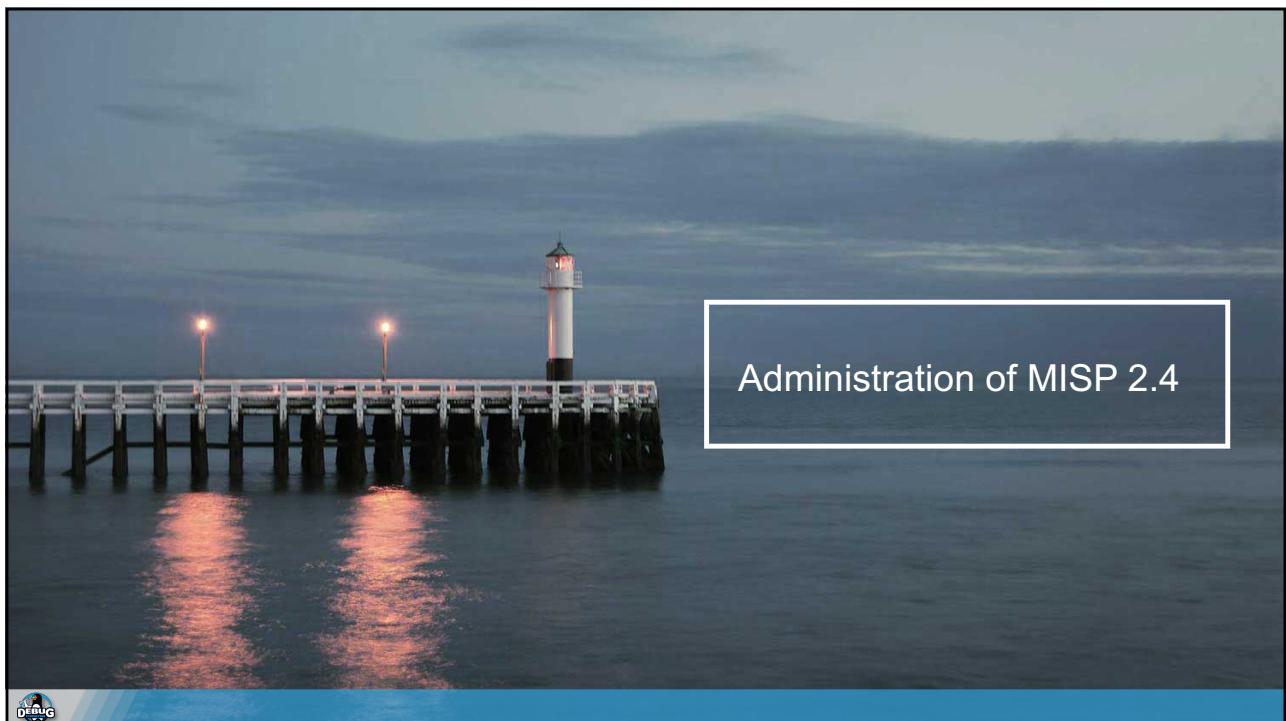
- Download an event
- Quick glance at the APIs
- Download search results
- ReST API and query builder



## MISP - Shorthand admin (if no admin training)

- Settings
- Troubleshooting
- Workers
- Logs





## MISP - Administration

- User and Organisation administration
- Sharing group creation
- Templates
- Tags and Taxonomy
- Whitelisting and Regexp entries
- Setting up the synchronisation
- Scheduled tasks
- Feeds
- Settings and diagnostics
- Logging
- Troubleshooting and updating



## MISP - Creating Users

- Add new user
- NIDS SID, Organisation, disable user
- Fetch the PGP key Roles
  - Re-using standard roles
  - Creating a new custom role
- Send out credentials



## MISP - Creating Organisations

- Adding a new organisation
- UUID
- Local vs External organisation
- Making an organisation self sustaining with Org Admins
- Creating a sync user



## MISP - Setting up the synchronisation

- Requirements - versions
- Pull/Push
- One way vs Two way synchronisation
- Exchanging sync users
- Certificates Filtering
- Connection test tool
- Previewing an instance
- Cherry picking and keeping the list updated



## MISP - Scheduled tasks

- How to schedule the next execution
- Frequency, next execution
- What happens if a job fails?



## MISP - Setting up the synchronisation

- MISP Feeds and their generation
- PyMISP
- Default free feeds
- Enabling a feed
- Previewing a feed and cherry picking
- Feed filters



## MISP - Settings and diagnostics

- Settings interface
- The tabs explained at a glance
- Issues and their severity
- Setting guidance and how to best use it



## MISP - Settings and diagnostics continued

- Basic instance setup
- Additional features released as hotfixes
- Customise the look and feel of your MISP
- Default behaviour (encryption, e-mailing, default distributions)
- Maintenance mode
- Disabling the e-mail alerts for an initial sync



## MISP - Settings and diagnostics continued

- Diagnostics
  - Updating MISP
  - Writeable Directories
  - PHP settings
  - Dependency diagnostics



## MISP - Settings and diagnostics continued

- Workers
- What do the background workers do?
- Queues
- Restarting workers, adding workers, removing workers
- Worker diagnostics (queue size, jobs page)
- Clearing worker queues
- Worker and background job debugging



## MISP - Logging

- Audit logs in MISP
- Enable IP logging / API logging
- Search the logs, the fields explained
- External logs
  - /var/www/MISP/app/tmp/logs/error.log
  - /var/www/MISP/app/tmp/logs/resque-worker-error.log
  - /var/www/MISP/app/tmp/logs/resque-scheduler-error.log
  - /var/www/MISP/app/tmp/logs/resque-[date].log
  - /var/www/MISP/app/tmp/logs/error.log apache access logs



## MISP - Updating MISP

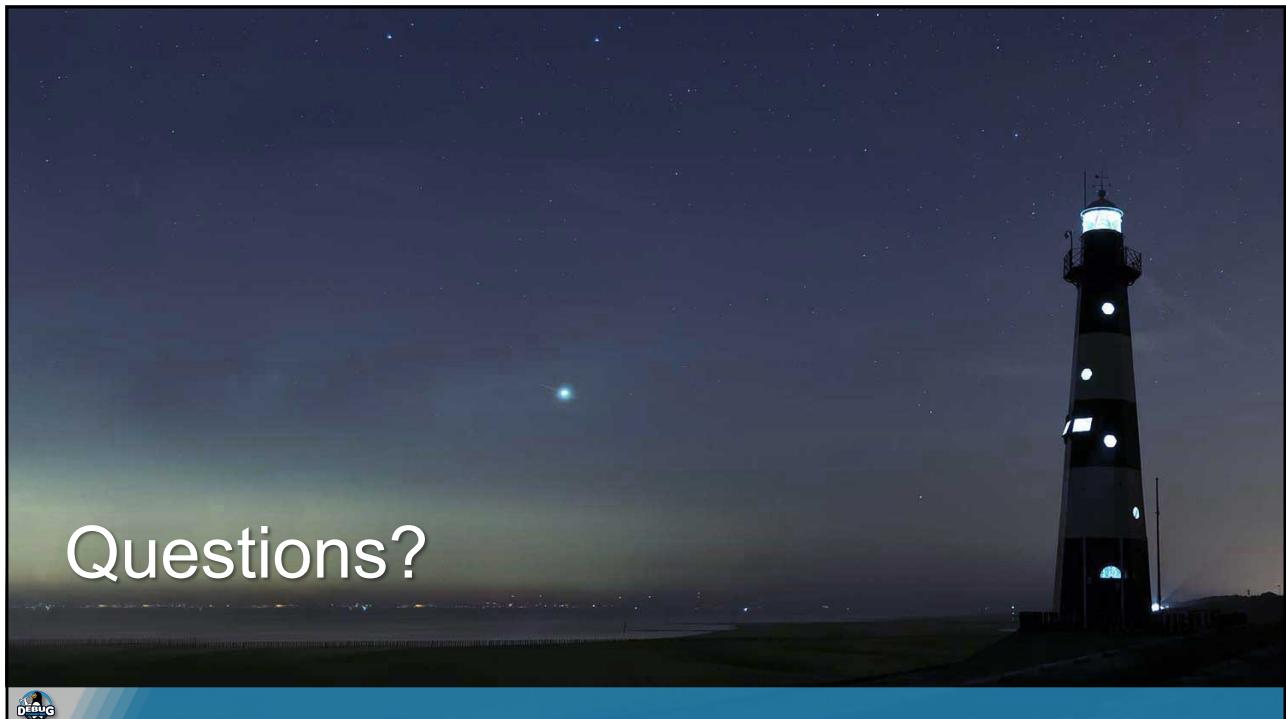
- git pull
- git submodule init && git submodule update
- reset the permissions if it goes wrong according to the INSTALL.txt
- when MISP complains about missing fields, make sure to clear the caches
  - in /var/www/MISP/app/tmp/cache/models remove myapp\*
  - in /var/www/MISP/app/tmp/cache/persistent remove myapp\*
- No additional action required on hotfix level
- Read the migration guide for major and minor version changes



## MISP - Administrative tools

- Upgrade scripts for minor / major versions
- Maintenance scripts





Questions?

