



การประชุมสัมมนาแลกเปลี่ยนเรียนรู้ เรื่อง การสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)

Department of Water Resources



www.dwr.go.th

27 พฤษภาคม 2568



นายโอกาส ถาวร
รองอธิบดีกรมทรัพยากรน้ำ
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO)



CONTENTS

1

การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์
ของกรมทรัพยากรน้ำ (Current status)

1.1

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษา
ความมั่นคงปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ พ.ศ. 2568

1.2

ผลการติดตั้ง Endpoint Detection and Response
(EDR)

1.3

ผลการประเมินระดับการเตรียมพร้อมและการปรับตัว (Cyber
Resilience Assessment)

1.4

การเชื่อมต่อแพลตฟอร์ม Malware Information Sharing
Platform หรือ MISP

1.5

การตรวจสอบและประเมินช่องโหว่ (Vulnerability Assessment)
และทำการทดสอบเจาะระบบ (Penetration Testing)

2

ปัญหาและอุปสรรค (Pain Points)

2.1

ขาดบุคลากรที่มีความเชี่ยวชาญเฉพาะด้านความมั่นคง
ปลอดภัยไซเบอร์

2.2

งบประมาณโครงการด้านความมั่นคงปลอดภัยไซเบอร์
ไม่ได้รับการจัดสรรอย่างต่อเนื่อง

2.3

ความตระหนักรู้ของบุคลากรภายในองค์กร เกี่ยวกับด้าน
ความมั่นคงปลอดภัยไซเบอร์

2.4

ระบบ IT ที่เก่าและมีความล้าสมัย

2.5

พัฒนาการและความหลากหลายของภัยคุกคาม



1 การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ของกรมทรัพยากรน้ำ (CURRENT STATUS)

1.1 ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ พ.ศ. 2568

ส่วนที่ 1 ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

- 1) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- 2) การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- 3) แผนการรับมือภัยคุกคามทางไซเบอร์

ส่วนที่ 2 กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

- 1) การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สิน และชีวิต ร่างกายของบุคคล (Identify)
- 2) มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)
- 3) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)
- 4) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)
- 5) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

หมายเหตุ:

คณะกรรมการบริหารเทคโนโลยีสารสนเทศระดับสูงของกรมทรัพยากรน้ำ ได้มีมติเห็นชอบ (ร่าง) ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมทรัพยากรน้ำ พ.ศ. 2568 ในวันจันทร์ที่ 21 เมษายน 2568 และอธิบดีกรมทรัพยากรน้ำได้ลงนามในประกาศดังกล่าวแล้ว ในวันที่ 14 พฤษภาคม 2568





1 การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ของกรมทรัพยากรน้ำ (CURRENT STATUS)

1.2 ผลการดำเนินงานของ ENDPOINT DETECTION AND RESPONSE (EDR)

IBM ReaQta (ดำเนินการโดยกรมทรัพยากรน้ำ)

มีการติดตั้ง EDR ยี่ห้อ IBM ReaQta จำนวน 450 Endpoints

โดยแบ่งเป็น กลุ่ม Server จำนวน 22 Endpoints และกลุ่ม Client จำนวน 428 Endpoints

ผลการดำเนินการของระบบ EDR ตั้งแต่เดือน เมษายน 2567 - เมษายน 2568 มีการตรวจจับสิ่งที่อาจจะก่อให้เกิดภัยคุกคามต่อระบบ จำนวน 49,511 รายการ โดยแบ่งเป็น

- ระดับภัยคุกคามเริ่มต้น จำนวน 45,362 รายการ ซึ่งไม่เป็นภัยต่อองค์กร
- และภัยคุกคามระดับที่เป็นอันตรายต่อระบบภายในองค์กร (Malicious) จำนวน 4,149 รายการ โดยระบบฯ ได้ดำเนินการ Kill Process กระบวนการที่คาดว่าจะเป็ภัยคุกคาม และลบไฟล์ที่ต้องสงสัยตาม Path ที่ระบบฯ ตรวจจับได้

SentinelOne (ได้รับความร่วมมือจาก สกมช.)

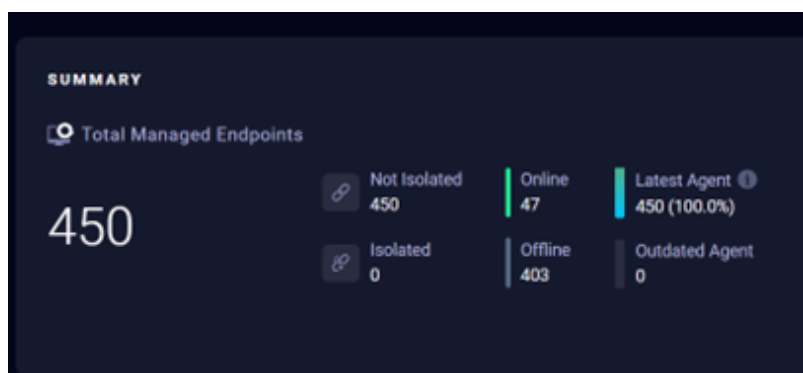
มีการติดตั้ง EDR ยี่ห้อ SentinelOne จำนวน 200 Endpoints โดยประกอบไปด้วยเครื่อง PC ทั้งส่วนกลางและส่วนภูมิภาค

โดยกรมทรัพยากรน้ำมีแผนติดตั้งให้ได้จำนวน 300 Endpoints ภายในสิ้นเดือนพฤษภาคมนี้

ปัจจุบันตรวจพบสิ่งที่คาดว่าเป็นภัยคุกคาม จำนวนกว่า 200 รายการ

กรมทรัพยากรน้ำ ได้มีการประสานงานและตรวจสอบเคสที่เกิดขึ้นกับทีมงาน SOC อย่างสม่ำเสมอ ว่าเป็นภัยคุกคามจริง หรือเป็นการใช้งานปกติของหน่วยงาน (False Positive)

หากเป็นภัยคุกคามจริง กรมทรัพยากรน้ำได้ดำเนินการป้องกันและแก้ไขตามคำแนะนำของ สกมช.





1 การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ของกรมทรัพยากรน้ำ (CURRENT STATUS)

1.3 ผลการประเมินระดับการเตรียมพร้อมและการปรับตัว (CYBER RESILIENCE ASSESSMENT)

ส่วนที่ 1 การประเมินความเสี่ยงตั้งต้นด้านไซเบอร์ (Inherent Risk Assessment – IRA)

ปัจจัยเสี่ยง	ระดับความเสี่ยง			ผลรวมการประเมินแต่ละปัจจัยเสี่ยง
	ต่ำ	ปานกลาง	สูง	
IR 1: เทคโนโลยีและการเชื่อมต่อ	7	3	9	สูง
IR 2: ช่องทางการให้บริการ	0	3	3	ปานกลาง
IR 3: ลักษณะผลิตภัณฑ์และการให้บริการ	0	0	2	สูง
IR 4: ลักษณะเฉพาะขององค์กร	0	3	1	ปานกลาง
IR 5: ประวัติการถูกคุกคามทางไซเบอร์	0	2	0	ปานกลาง

ผลรวมระดับความเสี่ยงตั้งต้น

ปานกลาง

มาตรการควบคุมที่พึงมี

หน่วยงานควรปฏิบัติได้ตามมาตรการที่กำหนดไว้สำหรับ Maturity Level ระดับ Baseline และระดับ Intermediate ที่กำหนดทุกข้อ



1 การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ของกรมทรัพยากรน้ำ (CURRENT STATUS)

1.3 ผลการประเมินระดับการเตรียมพร้อมและการปรับตัว (CYBER RESILIENCE ASSESSMENT)

ส่วนที่ 2 การประเมินระดับการจัดการภัยคุกคามทางไซเบอร์ (Maturity Assessment - MA)

การบริหารจัดการ ความเสี่ยง	รวม	ผลการประเมินการบริหารจัดการความเสี่ยง				
		Pass	Not Pass	Partially Pass	Alternative Control	Not Applicable
D1: การกำกับดูแล (Governance)	39	10	4	12	0	13
Baseline	13	8	1	4	0	0
Intermediate	13	2	3	8	0	0
Advanced	13	0	0	0	0	13
D2: การระบุความเสี่ยง (Identification)	17	5	6	3	0	3
Baseline	12	5	5	2	0	0
Intermediate	2	0	1	1	0	0
Advanced	3	0	0	0	0	3

การบริหารจัดการ ความเสี่ยง	รวม	ผลการประเมินการบริหารจัดการความเสี่ยง				
		Pass	Not Pass	Partially Pass	Alternative Control	Not Applicable
D3: การป้องกันความ เสี่ยง (Protection)	78	30	23	12	1	12
Baseline	55	27	18	9	1	0
Intermediate	11	3	5	3	0	0
Advanced	12	0	0	0	0	12
D4: การตรวจจับ (Detection)	38	14	6	6	0	12
Baseline	16	11	1	4	0	0
Intermediate	10	3	5	2	0	0
Advanced	12	0	0	0	0	12

การบริหารจัดการ ความเสี่ยง	รวม	ผลการประเมินการบริหารจัดการความเสี่ยง				
		Pass	Not Pass	Partially Pass	Alternative Control	Not Applicable
D5: การตอบสนองต่อ เหตุการณ์และการกู้คืน ระบบ (Response and Recovery)	15	3	5	5	0	2
Baseline	10	2	4	4	0	0
Intermediate	3	1	1	1	0	0
Advanced	2	0	0	0	0	2
D6: การบริหารความ เสี่ยงจากบุคคลภายนอก (Third Party Risk Management)	19	7	7	2	0	3
Baseline	13	7	4	2	0	0
Intermediate	3	0	3	0	0	0
Advanced	3	0	0	0	0	3

Pass = ผ่าน/ดำเนินการแล้ว

Not Pass = ไม่ผ่าน/ไม่ได้ดำเนินการ

Partially Pass = ผ่านบางส่วน/ดำเนินการบางส่วน

Alternative Control = ไม่มีการดำเนินการตามที่มาตรการกำหนด
แต่มีอย่างอื่นที่สามารถทดแทนได้

Not Applicable = ไม่เกี่ยวข้อง หรือ ไม่จำเป็นต้องประเมินในส่วนนี้

ผลสรุป (จากทั้งหมด 206 ข้อ)

Pass : 69

Not Pass : 51

Partially Pass : 40

Alternative Control : 1

Not Applicable : 45



1

การดำเนินงานด้านความมั่นคงปลอดภัย ไซเบอร์ของกรมทรัพยากรน้ำ

การดำเนินงานภายใต้ความร่วมมือระหว่างกรมทรัพยากรน้ำ และ สกมช.

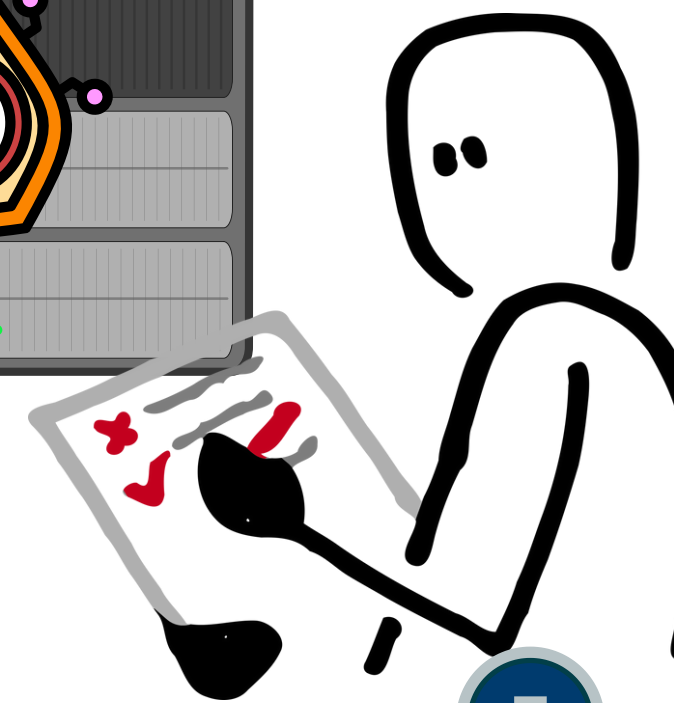
1.4 การเชื่อมต่อแพลตฟอร์มการแบ่งปันข้อมูลมลแวร์ (MALWARE INFORMATION SHARING PLATFORM) หรือ MISP



The screenshot shows the MISP web interface. At the top, there's a navigation bar with links like Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, and API. Below this, there's a 'Feeds' section with a sub-header 'Generate feed lookup caches or fetch feed data (enabled feeds only)'. There are buttons for 'Load default feed metadata', 'Cache all feeds', 'Cache freetext/CSV feeds', 'Cache MISP feeds', and 'Fetch and store all feed data'. A table lists various feeds with columns for ID, Enabled, Caching, Name, Format, Provider, Org, Source, and URL. The table includes feeds like CIRCL OSINT Feed, The Botvrij.eu Data, ELILO: IP Feed, blockrules of rules.emergingthreats.net, Tor exit nodes, Tor ALL nodes, cybercrime-tracker.net, Phishtank online valid phishing, ip-block-list - snort.org, diamondfox_panels, pop3gropers, Feodo IP Blocklist, OpenPhish url list, firehol_level1, and IPs from High-Confidence DGA-Based.

ID	Enabled	Caching	Name	Format	Provider	Org	Source	URL
1	✓	✓	CIRCL OSINT Feed	misp	CIRCL	network	https://www.circl.lu/doc/misp/feed-osint	
2	✓	✓	The Botvrij.eu Data	misp	Botvrij.eu	network	https://www.botvrij.eu/data/feed-osint	
3	✓	✓	ELILO: IP Feed (Community version)	freetext	elilio tech	network	https://cdn.elilio.tech/community-feed	New fixed
4	✓	✓	blockrules of rules.emergingthreats.net	csv	rules.emergingthreats.net	network	https://rules.emergingthreats.net/blockrules/compromised-ips.txt	New fixed
5	✓	✓	Tor exit nodes	csv	TOR Node List from dan.me.uk - careful, this feed applies a lock-out after each pull. This is shared with the "Tor ALL nodes" feed.	network	https://www.dan.me.uk/torlist7/exit	New fixed
6	✓	✓	Tor ALL nodes	csv	TOR Node List from dan.me.uk - careful, this feed applies a lock-out after each pull. This is shared with the "Tor exit nodes" feed.	network	https://www.dan.me.uk/torlist/	New fixed
7	✓	✓	cybercrime-tracker.net - all	freetext	cybercrime-tracker.net	network	https://cybercrime-tracker.net/all.php	New fixed
8	✓	✓	Phishtank online valid phishing	csv	Phishtank	network	https://data.phishtank.com/data/online-valid.csv	New fixed
9	✓	✓	ip-block-list - snort.org	freetext	https://snort.org	network	https://snort.org/downloads/ip-block-list	New fixed
10	✓	✓	diamondfox_panels	freetext	pan-unit42	network	https://raw.githubusercontent.com/pan-unit42/foes/master/diamondfox/diamondfox_panels.txt	New fixed
11	✓	✓	pop3gropers	csv	home.nuug.no	network	https://home.nuug.no/~peter/pop3gropers.txt	New fixed
12	✓	✓	Feodo IP Blocklist	csv	abuse.ch	network	https://feodo.abuse.ch/downloads/ipblocklist.csv	New fixed
13	✓	✓	OpenPhish url list	freetext	openphish.com	network	https://raw.githubusercontent.com/openphish/public_feed/refs/heads/main/feed.txt	New fixed
14	✓	✓	firehol_level1	freetext	iplists.firehol.org	network	https://raw.githubusercontent.com/itsaou/blocklist-ipsets/master/firehol_level1.netset	New fixed
15	✓	✓	IPs from High-Confidence DGA-Based	csv	osint.bambenekconsulting.com	network	https://osint.bambenekconsulting.com/feeds/c2-ipmasterlist-high.txt	New fixed

1.5 การสแกนหาช่องโหว่ (VULNERABILITY ASSESSMENT) และทดสอบเจาะระบบ (PENETRATION TESTING)



สกมช. จะเข้ามาดำเนินการ
ระหว่างวันที่ 26 - 30 พฤษภาคม 2568



2

ปัญหา อุปสรรคและผลตอบรับที่หน่วยงานพบเจอ เมื่อดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (PAIN POINTS)

2.1

ขาดบุคลากรที่มีความเชี่ยวชาญเฉพาะด้านความมั่นคงปลอดภัยไซเบอร์

2.2

งบประมาณโครงการด้านความมั่นคงปลอดภัยไซเบอร์ ไม่ได้รับการจัดสรรอย่างต่อเนื่อง

2.3

ความตระหนักรู้ของบุคลากรภายในองค์กร เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์

2.4

ระบบ IT ที่เก่าและมีความล้าสมัย

2.5

พัฒนาการและความหลากหลายของภัยคุกคาม