รายงานสรุปผลการปฏิบัติงาน

การให้บริการดูแลรักษาความมั่นคงปลอดภัยทางไซเบอร์

(Cyber SecurityOperation Center)

ประจำวันที่ 1 กุมภาพันธ์ - 28 กุมภาพันธ์ 2569

สำหรับ

โรงพยาบาลบ้านคา

จังหวัดราชบุรี

จัดทำโดย

บริษัท ซีเคียวริตี้ ไลฟ์ ไซเคิล จำกัด

สารบัญ

หัวข้อ **หน้า**

รายงานสรุปผลการดำเนินงานของระบบการให้บริการดูแลรักษาความมั่นคงปลอดภัยทางไซเบอร์
ประจำวันที่ 1 กุมภาพันธ์ - 28 กุมภาพันธ์ 2569
เสนอ
โรงพยาบาลบ้านคา จังหวัดราชบุรี
จัดทำโดย บริษัท ซีเคียวริตี้ ไลฟ์ ไซเคิล จำกัด

หลักการและเหตุผล

ในยุคปัจจุบัน การใช้งานเทคโนโลยีสารสนเทศและการสื่อสารผ่านเครือข่ายอินเทอร์เน็ตได้เข้ามามีบทบาทสำคัญต่อการดำเนินงานในทุกภาคส่วน ทั้งในภาครัฐและเอกชน การพัฒนาทางด้านเทคโนโลยีดังกล่าว แม้จะส่งผลให้เกิดความสะดวกสบายในการติดต่อสื่อสารและการบริหารจัดการข้อมูล แต่ก็ได้นำมาซึ่งความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ ซึ่งมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง ทั้งในรูปแบบของการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การโจรกรรมข้อมูล การโจมตีระบบเพื่อก่อกวน หรือการแพร่กระจายของซอฟต์แวร์ที่เป็นอันตราย ความมั่นคงปลอดภัยทางไซเบอร์จึงเป็นปัจจัยสำคัญในการรักษาความปลอดภัยของข้อมูลและทรัพย์สินทางดิจิทัล ซึ่งเป็นสิ่งที่จำเป็นอย่างยิ่งต่อการดำเนินงานขององค์กร หากไม่มีมาตรการที่เพียงพอในการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ อาจส่งผลให้เกิดความเสียหายต่อการดำเนินงาน ความเชื่อมั่นของประชาชน รวมถึงความปลอดภัยของข้อมูลส่วนบุคคล ซึ่งอาจนำไปสู่ผลกระทบทางกฎหมายและการเสียหายทางธุรกิจที่รุนแรง

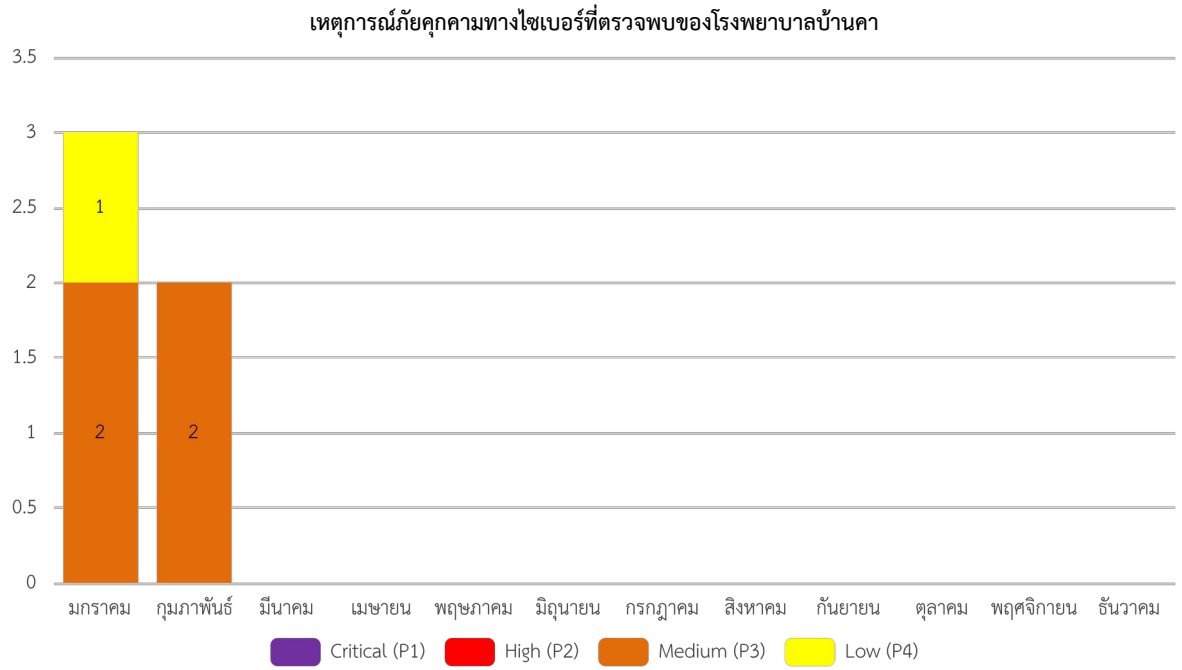
การให้บริการความมั่นคงปลอดภัยทางไซเบอร์จึงเป็นสิ่งที่จำเป็นต้องได้รับการพัฒนาและส่งเสริมอย่างจริงจัง โดยมุ่งเน้นการป้องกันและลดความเสี่ยงจากการโจมตีทางไซเบอร์ ผ่านการใช้เทคโนโลยีที่ทันสมัย การจัดทำมาตรการรักษาความปลอดภัยที่สอดคล้องกับมาตรฐานสากล และการพัฒนาศักยภาพของบุคลากรในด้านการรักษาความปลอดภัยทางไซเบอร์ การดำเนินการดังกล่าวมีความจำเป็นที่จะต้องมีหน่วยงานที่สามารถประสานงาน ให้ความรู้ และช่วยเสริมสร้างให้ระบบงาน บุคลากร ไปจนถึงภาพรวมของหน่วยงานมีความมั่นคงปลอดภัยสารสนเทศที่เพิ่มมากขึ้น โดยอ้างอิงมาตรฐานสากลเพื่อให้มีความน่าเชื่อถือ และสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศของหน่วยงานให้ยั่งยืนต่อไป

วัตถุประสงค์

เพื่อให้มั่นใจว่าเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นจะได้รับการเฝ้าระวังและแจ้งเตือนได้อย่างมีประสิทธิภาพ ตรงตามขอบเขตการดำเนินงานที่บริษัทฯ ได้รับมอบหมายภายในสัญญาภายใต้โครงการฯ การปฏิบัติและดำเนินงานจะต้องเป็นไปอย่างถูกต้องครบถ้วนตามขอบเขตของข้อกำหนดในโครงการฯ

บทสรุปผู้บริหาร

บริษัทฯ ได้สรุปเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ส่งผลต่อความปลอดภัยของระบบคอมพิวเตอร์และสารสนเทศที่เกิดขึ้นประจำปี 2569 ทั้งหมด 5 เหตุการณ์ โดยมีรายละเอียดดังนี้



1. **ภาพรวมของการเฝ้าระวังเหตุการณ์ภัยคุกคามทางไซเบอร์ (Security Incident)**

   1.1. **ผลการเฝ้าระวังประจำวันที่ 1 กุมภาพันธ์ - 28 กุมภาพันธ์ 2569ตรวจพบเหตุการณ์ที่สำคัญดังรายละเอียดต่อไปนี้**

โรงพยาบาล	จำนวนเหตุการณ์	Critical	High	Medium	Low
โรงพยาบาลบ้านคา	2	0	0	2	0

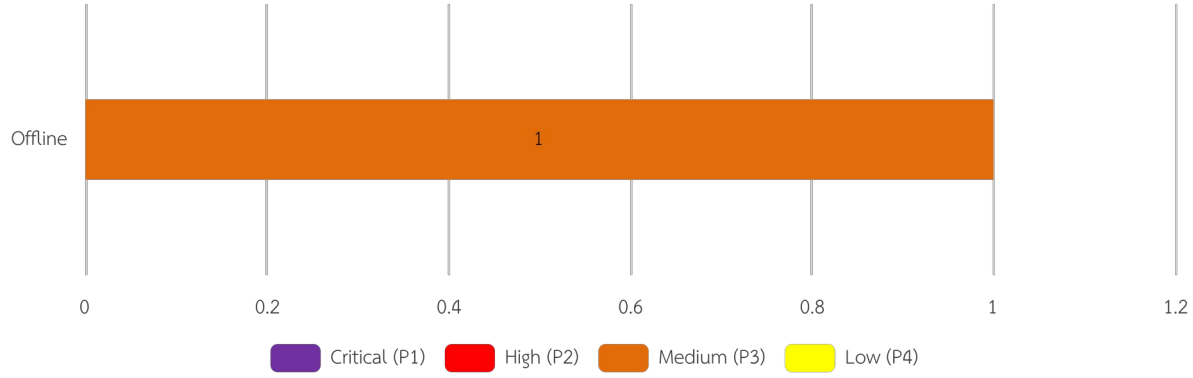
   1.2. **สรุปเหตุการณ์ภัยคุกคามทางไซเบอร์คงค้างประจำปี 2569 ประจำวันที่ 1 กุมภาพันธ์ - 28 กุมภาพันธ์ 2569**
   ไม่พบเหตุการณ์คงค้าง

2. เหตุการณ์ภัยคุกคามทางไซเบอร์ที่น่าสนใจ

2.1. ตรวจพบเหตุการณ์ผ่าน Endpoint Detection and Response (EDR) ไม่พบเหตุการณ์ผิดปกติ

2.2. ตรวจพบเหตุการณ์ผ่าน Next-generationAntivirus (NGAV) พบ 1เหตุการณ์ดังนี้

ภัยคุกคามจากการตรวจจับผ่านระบบNext-generation(NGAV)

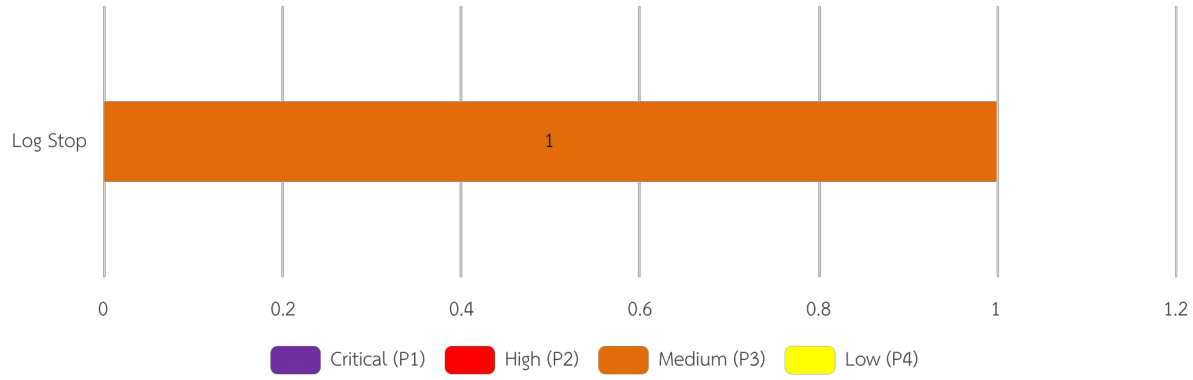


2.2.1. Offline จำนวน 1 เหตุการณ์

Private IP Address	Mac Address	Host Name	Response Time	Action	Priority
192.168.40.25	00:0c:29:b6:88:fc	DESKTOP-921DQPG	2026-02-09 21:00:37	Detection	Medium (P3)

2.3. ตรวจพบเหตุการณ์ผ่านSecurity Information and Event Management (SIEM) พบ 1 เหตุการณ์ ดังนี้

ภัยคุกคามจากการตรวจจับผ่าน Security Information and Event Management (SIEM)



2.3.1. Log Stop จำนวน 1 เหตุการณ์

Private IP	Host Name	Category	Response Time	Priority
192.168.60.8	localhost.localdomain	vCenter Latest Event: 20:15:54, Mon, Feb 09 2026	2026-02-10 21:00:24	Medium (P3)

2.4. ตรวจพบการใช้งาน Port ที่ไม่ได้รับอนุญาต ไม่พบเหตุการณ์ผิดปกติ

No	VM Name	Public IP	Port (ได้รับการยืนยันจากโรงพยาบาลแล้ว)
1	-	203.157.226.196	-

No	VM Name	Public IP	Port (ได้รับการยืนยันจากโรงพยาบาลแล้ว)
2	-	203.157.226.198	-
3	-	203.157.226.194	-
4	-	203.157.226.195	-
5	-	203.157.226.197	-
6	-	1.20.137.209	10443
7	-	203.157.226.192	-
8	-	203.157.226.193	80,443

หมายเหตุ: ดำเนินการเฉพาะเครื่องอุปกรณ์ที่ทางโรงพยาบาลแจ้งเท่านั้น โดย Port ที่เสี่ยงการโดนโจมตีปัจจุบันได้แก่21, 22, 23 , 80, 445, 1433, 1434, 3306, 3389, 5432, 5900

2.5. ตรวจพบการใช้งาน Backup ที่ไม่มีการอัปโหลดไฟล์ ไม่พบเหตุการณ์ผิดปกติ

VM Name	Report On	จำนวนไฟล์ที่สำเร็จ	จำนวนไฟล์ที่ไม่สำเร็จ	สถานะการสำรองข้อมูล
DESKTOP-0UKEG02	2026-02-01	1	0	SUCCESS
DESKTOP-0UKEG02	2026-02-02	1	0	SUCCESS
DESKTOP-0UKEG02	2026-02-03	1	0	SUCCESS
DESKTOP-0UKEG02	2026-02-04	1	0	SUCCESS
DESKTOP-0UKEG02	2026-02-05	1	0	SUCCESS
DESKTOP-0UKEG02	2026-02-06	1	0	SUCCESS
DESKTOP-0UKEG02	2026-02-07	1	0	SUCCESS
DESKTOP-0UKEG02	2026-02-08	1	0	SUCCESS
DESKTOP-0UKEG02	2026-02-09	1	0	SUCCESS
DESKTOP-0UKEG02	2026-02-10	1	0	SUCCESS
DESKTOP-0UKEG02	2026-02-11	1	0	SUCCESS
DESKTOP-0UKEG02	2026-02-12	1	0	SUCCESS
DESKTOP-0UKEG02	2026-02-17	1	0	SUCCESS
DESKTOP-0UKEG02	2026-02-18	1	0	SUCCESS
DESKTOP-0UK	2026-02-19	1	0	SUCCESS

VM Name	Report On	จำนวนไฟล์ที่สำเร็จ	จำนวนไฟล์ที่ไม่สำเร็จ	สถานะการสำรองข้อมูล
EG02				
DESKTOP-0UK EG02	2026-02-20	1	0	SUCCESS
DESKTOP-0UK EG02	2026-02-21	1	0	SUCCESS
DESKTOP-0UK EG02	2026-02-22	1	0	SUCCESS
DESKTOP-0UK EG02	2026-02-23	1	0	SUCCESS
DESKTOP-0UK EG02	2026-02-24	1	0	SUCCESS
DESKTOP-0UK EG02	2026-02-25	1	0	SUCCESS
DESKTOP-0UK EG02	2026-02-26	1	0	SUCCESS
DESKTOP-0UK EG02	2026-02-27	1	0	SUCCESS
DESKTOP-0UK EG02	2026-02-28	1	0	SUCCESS

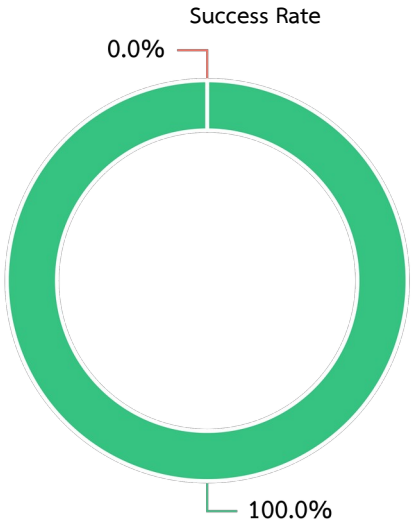
หมายเหตุ
Success: สำเร็จ
Fail: ไม่สำเร็จ
Not installed: ไม่ได้มีการติดตั้ง

2.6. ตรวจพบการใช้งาน Multi-Factor Authentication (2FA) ไม่พบเหตุการณ์ผิดปกติ

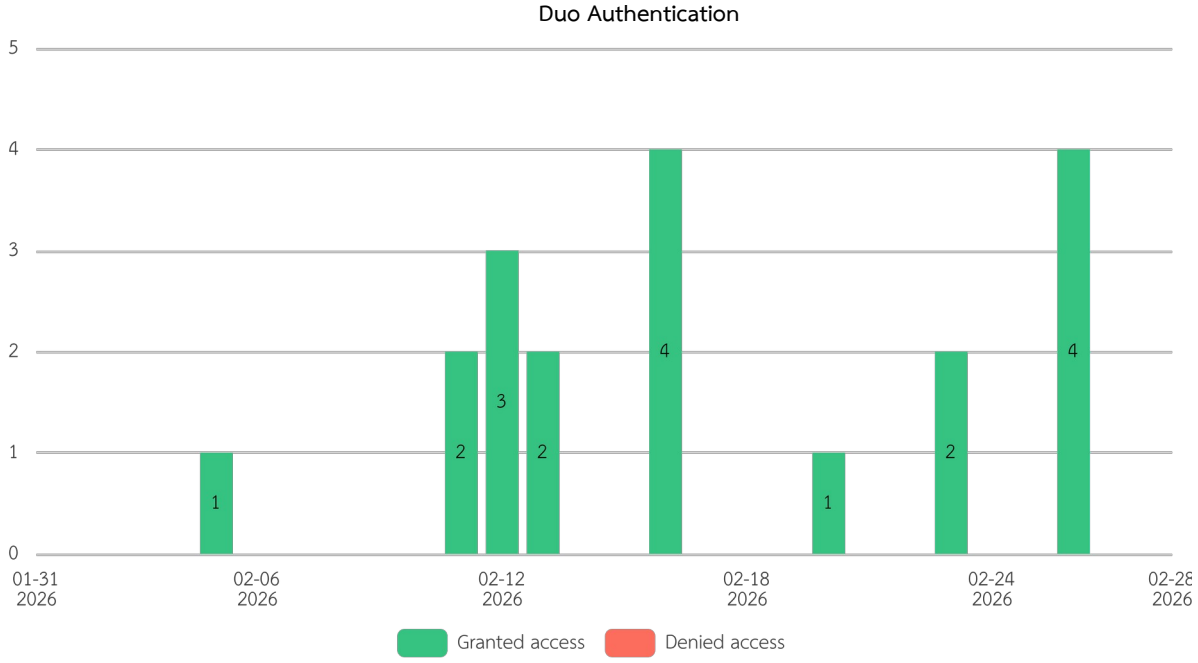
2.7. ตรวจพบการใช้งาน Web Application Firewall (WAF) ไม่พบเหตุการณ์ผิดปกติ

2.8. รายงานการใช้งานระบบ Multi-Factor Authentication (2FA)

2.8.1. Success Rate

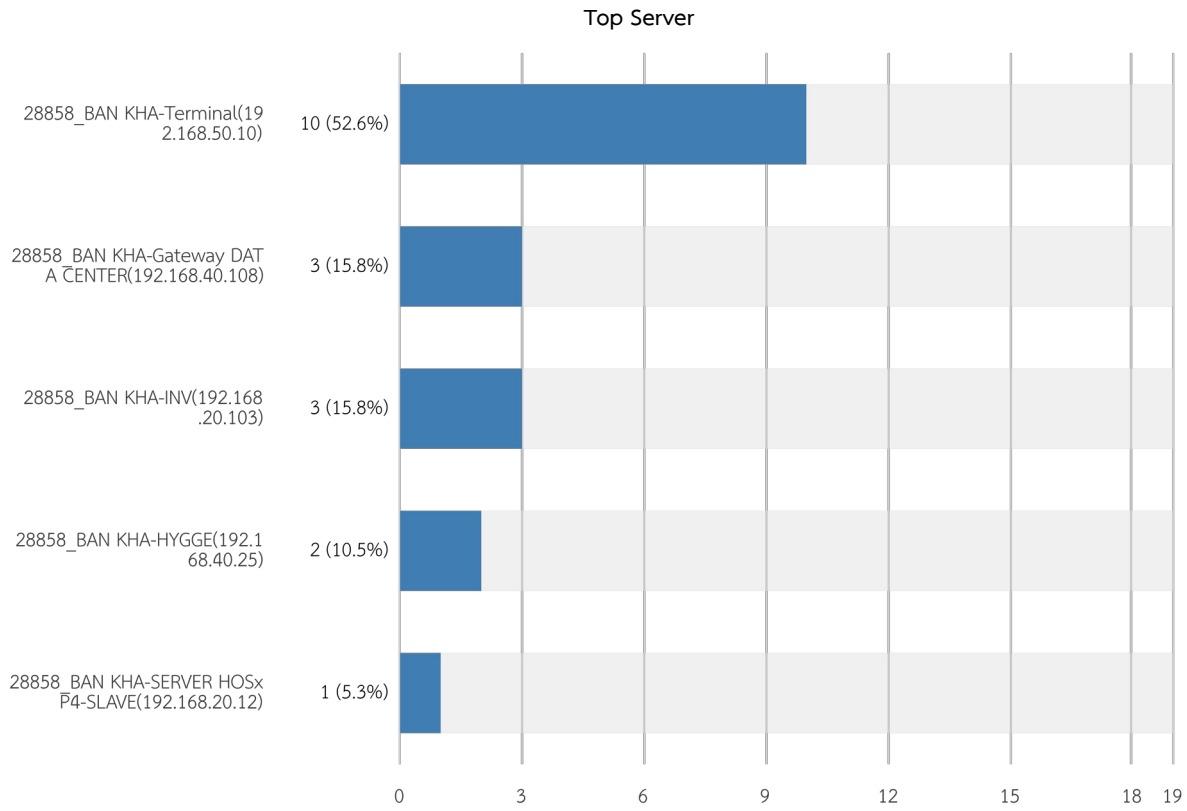


2.8.2. Duo Authentication

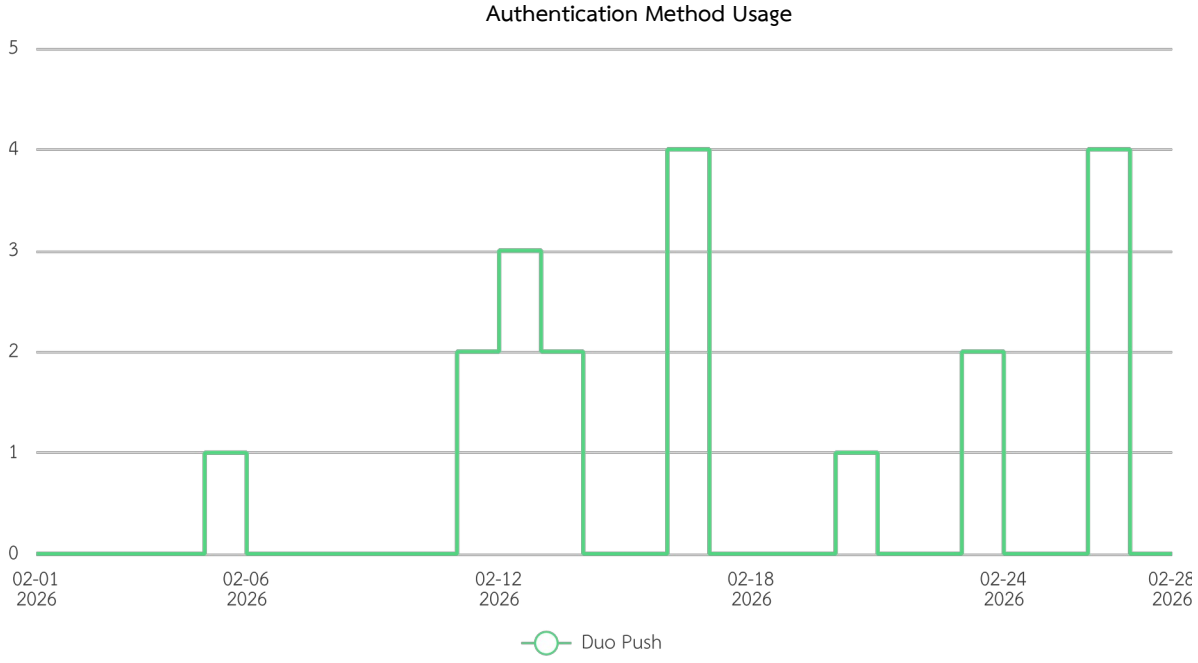


2.8.3. Authentication Methods

2.8.4. Top 10 Server



2.8.5. Authentication Methods Usage

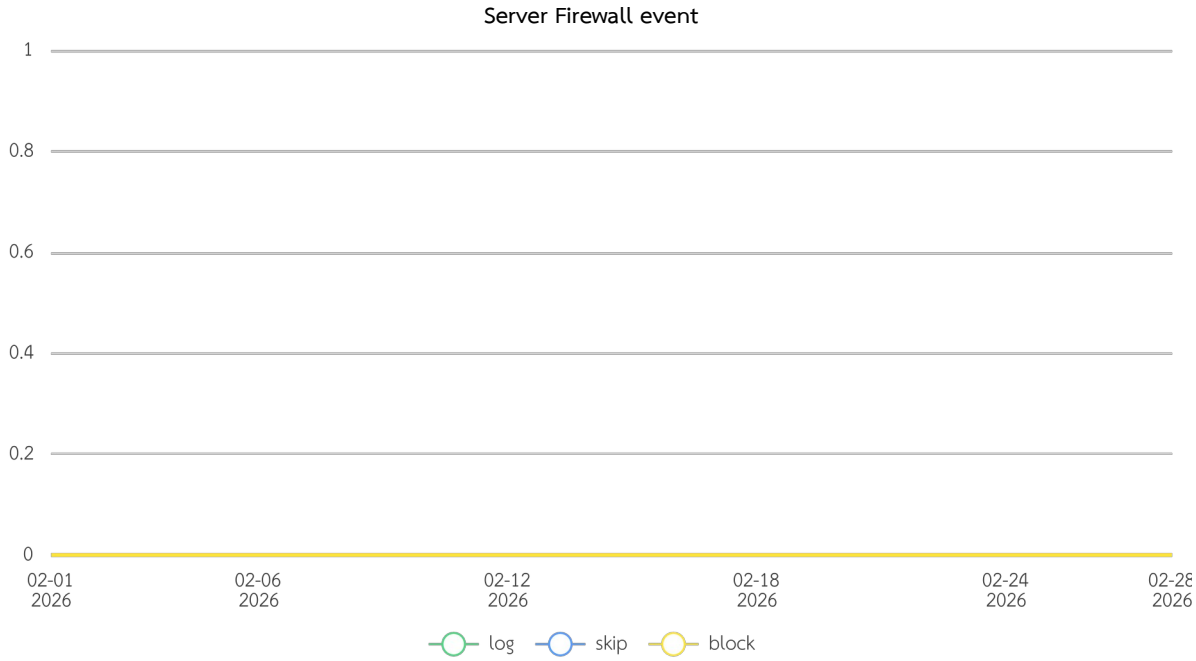


2.9. รายงานการเข้าใช้งาน Web Application Firewall (WAF)

โรงพยาบาล	Domain
โรงพยาบาลบ้านคา	bkhosp.moph.go.th

2.9.1. Server Firewall Events

Total	Log	block	Skip
0	0	0	0



2.9.2. Top 10 event by source

2.9.2.1. Source IP Address: ไม่พบข้อมูล

2.9.2.2. User Agent: ไม่พบข้อมูล

2.9.2.3. Paths: ไม่พบข้อมูล

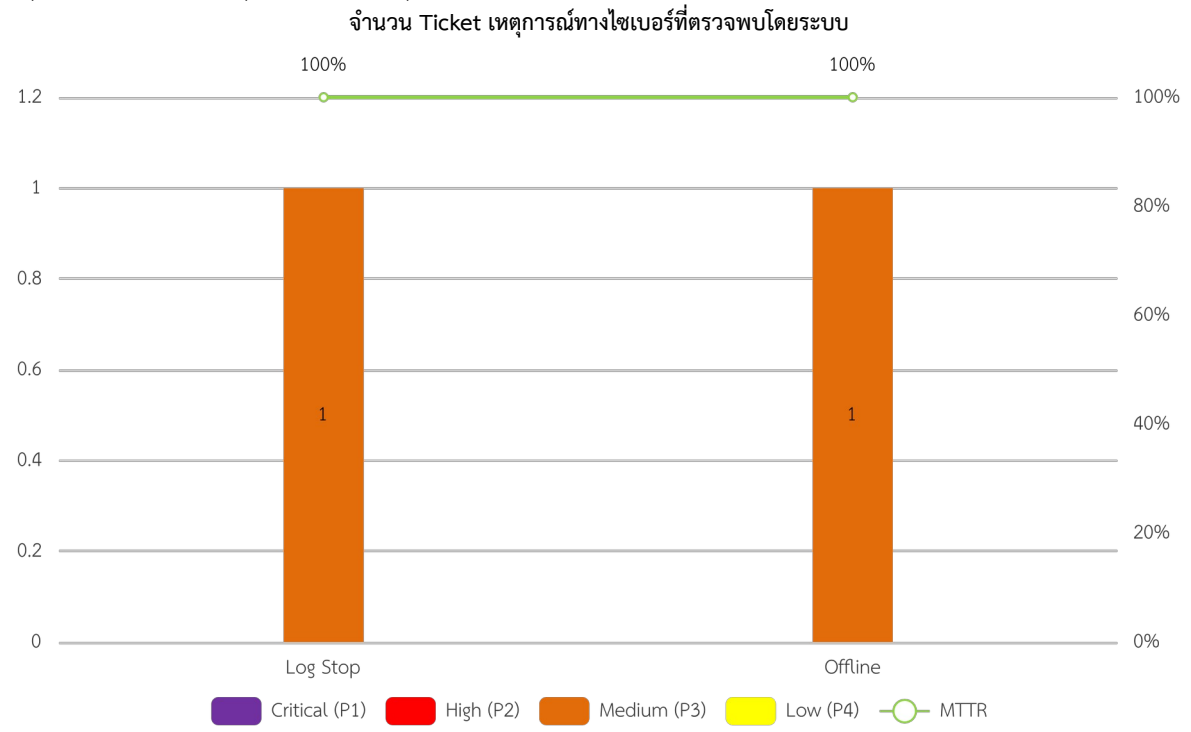
2.9.2.4. Countries: ไม่พบข้อมูล

2.9.2.5. Host: ไม่พบข้อมูล

2.9.2.6. Source ASNs: ไม่พบข้อมูล

3. จำนวนเหตุการณ์ที่ตรวจพบประจำวันที่ 1 กุมภาพันธ์ - 28 กุมภาพันธ์ 2569

กราฟแสดงจำนวน Ticket และเปอร์เซ็นระยะเวลาการตอบสนองต่อเหตุการณ์ต่างๆ แบ่งตามลำดับประเภทของแต่ละเหตุการณ์ประจำวันที่ 1 กุมภาพันธ์ - 28 กุมภาพันธ์ 2569



สรุปจำนวนอุปกรณ์ที่ติดตั้ง

จำนวนอุปกรณ์ที่ติดตั้ง Endpoint Detection and Response (EDR)จำนวน 5 เครื่อง

No.	Hostname	OS Version	Private IP	Mac Address	Host Status	Last Active
1	BMS-Restore	CentOS 8.5	192.168.40.3	52-54-00-80-91-bb	online	2026-02-28 23:40:00
2	SGH725TPA1srv	CentOS 7.9	192.168.30.60	52-54-00-6b-c0-38	online	2026-02-28 23:29:00
3	HOSxP-Salve	AlmaLinux 8.10	192.168.20.12	52-54-00-5c-77-bc	online	2026-02-28 23:46:00
4	HOSxP-Master	AlmaLinux 9.5	192.168.20.11	bc-24-11-d5-15-a4	online	2026-02-28 23:45:00
5	InvServer	CentOS 7.5	192.168.20.103	52-54-00-27-48-9a	online	2026-02-28 23:24:00

จำนวนอุปกรณ์ที่ติดตั้ง ระบบ Next-generation Antivirus(NGAV)จำนวน 6เครื่อง

No.	Hostname	OS Version	Type	Private IP	Mac Address	Host Status	Last Active
1	DESKTOP-921DQPG	Windows 10	Server	192.168.40.25	00-0c-29-b6-88-fc	online	2026-02-28 11:49:00
2	DESKTOP-6SO3RER	Windows 10	Server	192.168.50.10	d0-50-99-9a-a4-96	online	2026-02-28 11:47:00
3	DESKTOP-0P9PF6V	Windows 11	Server	192.168.40.108	50-3e-aa-08-6d-07	online	2026-02-28 11:45:00
4	BMS-Restore	CentOS 7.9	Server	192.168.40.102	52-54-00-bc-37-03	online	2026-02-28 11:31:00
5	DESKTOP-IBEF7R3	Windows 10	Server	192.168.40.4	06-fe-fd-03-7b-cb	online	2026-02-28 11:40:00
6	WIN-K85VA7D6JRL	Windows Server 2019	Server	192.168.30.15	b8-cb-29-b3-de-68	online	2026-02-28 11:15:00

จำนวนอุปกรณีที่ติดตั้ง Security Information and Event Management (SIEM) จำนวน 5 เครื่อง

No.	Hostname	Category	Private IP	Event Status	Last Active
1	localhost.localdomain	VMware vCenter	192.168.60.8	SUCCESS	2026-02-28

No.	Hostname	Category	Private IP	Event Status	Last Active
					23:00:00
2	hosxp	Generic Unix	192.168.60.10	WARNING	2026-02-28 23:00:00
3	paperless	Generic Unix	192.168.60.7	WARNING	2026-02-28 23:00:00
4	HOSxP-Master	Generic Unix	192.168.20.11	WARNING	2026-02-28 23:00:00
5	Bankhahos-FortiGate-40F	Fortinet FortiOS	192.168.50.1	SUCCESS	2026-02-28 23:00:00