การป้องกันทางไซเบอร์

พ.ศ.๒๕๖๖

โดย
กองรักษาความมั่นคงปลอดภัยไซเบอร์
ศูนย์ไซเบอร์กองทัพอากาศ

บันทึกข้อความ

ส่วนราชการ ทสส.ทอ.(สนผ.โทร.๒-๒๔๖๗)

ที่ กห ๐๖๐๙.๓/ ๑๒๒๕ **วันที่** ๑๙ ก.ย.๖๖

เรื่อง ส่งคู่มือการฝึกงานในหน้าที่ จำพวกทหารไซเบอร์

เสนอ ศชบ.ทอ.

๑. ตามอนุมัติ จก.ทสส.ทอ.เมื่อ ๑๓ ก.ย.๖๖ ท้ายหนังสือ สนผ.ทสส.ทอ.ที่ กห ๐๖๐๙.๓(๒)/๒๐๓ ลง ๑๒ ก.ย.๖๖ ให้ใช้คู่มือการฝึกงานในหน้าที่ของจำพวกทหารไซเบอร์ สำหรับการฝึกความชำนาญของจำพวกทหารไซเบอร์ นั้น

๒. ทสส.ทอ.จึงขอส่งคู่มือการฝึกงานในหน้าที่ของจำพวกทหารไซเบอร์ เพื่อใช้ในการฝึกความชำนาญของจำพวกทหารไซเบอร์ รายละเอียดตามแนบ

จึงเสนอมาเพื่อดำเนินการต่อไป

พล.อ.ต.

ผอ.สนผ.ทสส.ทอ.ทำการแทน

จก.ทสส.ทอ.

บันทึกข้อความ

ส่วนราชการ สนผ.ทสส.ทอ.(กนผ.โทร.๒-๑๐๕๖)

ที่ กห ๐๖๐๙.๓(๒)/ ๒๐๓ **วันที่** ๑๒ ก.ย.๖๖

เรื่อง ขออนุมัติใช้คู่มือการฝึกงานในหน้าที่ จำพวกทหารไซเบอร์

เรียน จก.ทสส.ทอ.

๑. ตามหนังสือ ศชบ.ทอ.ที่ กห ๐๖๕๐.๑/๗๔๖ ลง ๒๘ ส.ค.๖๖ ขอให้พิจารณาตำราของหลักสูตรสายวิทยาการไซเบอร์ นั้น

๒. สนผ.ทสส.ทอ.ตรวจสอบแล้ว มีข้อมูล ดังนี้

๒.๑ ระเบียบ ทอ.ว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓ และฉบับแก้ไขเพิ่มเติม ข้อ ๓๑.๑๙ หนังสือคู่มือการฝึกงานในหน้าที่ เป็นเอกสารอธิบายความรู้ในวิทยาการและวิธีปฏิบัติงานของเหล่าทหารหรือจำพวกทหารซึ่งส่วนราชการหัวหน้าสายวิทยาการจัดทำขึ้น เพื่อใช้ประกอบการฝึกงานในหน้าที่ตามระดับความชำนาญ โดยมีความสัมพันธ์และสอดคล้องกับเรื่องและหัวข้อวิชาในมาตรฐานการฝึกความชำนาญ ให้เรียกโดยย่อว่า "หนังสือคู่มือการฝึก" และให้จัดทำตามผนวก ๗ แนบท้ายระเบียบนี้ (แนบ ๑)

๒.๒ ทสส.ทอ.เป็นหน่วยรับผิดชอบสายวิทยาการสารสนเทศและสงครามอิเล็กทรอนิกส์และสายวิทยาการไซเบอร์ ได้จัดทำคู่มือการฝึกงานในหน้าที่ เพื่อเพิ่มพูนความรู้ ความสามารถ และความชำนาญการปฏิบัติงานในสายวิทยาการไซเบอร์ จำนวน ๕ วิชา (แนบ ๒) ประกอบด้วย

๒.๒.๑ วิชา การป้องปรามทางไซเบอร์
๒.๒.๒ วิชา การป้องกันทางไซเบอร์
๒.๒.๓ วิชา การข่าวกรองทางไซเบอร์
๒.๒.๔ วิชา การพิสูจน์หลักฐานทางดิจิทัล
๒.๒.๕ วิชา ความรู้พื้นฐานสำหรับปฏิบัติการทางไซเบอร์

๓. สนผ.ฯ พิจารณาแล้ว เพื่อให้การดำเนินการฝึกงานในหน้าที่ของสายวิทยาการไซเบอร์เป็นไปด้วยความเรียบร้อย จึงขออนุมัติใช้คู่มือการฝึกงานในหน้าที่ของจำพวกทหารไซเบอร์ สำหรับการฝึกความชำนาญของจำพวกทหารไซเบอร์ต่อไป

จึงเรียนมาเพื่ออนุมัติตามข้อ ๓

พล.อ.ต.
ผอ.สนผ.ทสส.ทอ.

- อนุมัติตามข้อ ๓

พล.อ.ท.
จก.ทสส.ทอ.
๑๙ ก.ย.๖๖

ทสส.ทอ.
เลขรับ ๕๕๔๐
วันที่ ๒๔ ส.ค. ๒๕๖๖
เวลา ๑๓๔๘

บันทึกข้อความ

ส่วนราชการ ศชบ.ทอ.(นกพ.ฯ โทร.๒-๒๗๑๒)

ที่ กห ๐๖๕๐.๑/ ๗๔๖ วันที่ ๒๔ ส.ค.๖๖

เรื่อง ขอให้พิจารณาตำราของหลักสูตรสายวิทยาการไซเบอร์

สนผ.ทสส.ทอ.
เลขรับ ๒๗๗๑
วันที่ ๒๔ ส.ค.๖๖
เวลา ๑๓๕๗

เสนอ ทสส.ทอ.

สนผ-๖
๒๔ ส.ค. ๒๕๖๖

๑. ตามหนังสือ ทสส.ทอ.ที่ กห ๐๖๐๙.๓/๑๐๘๙ ลง ๙ ส.ค.๖๖ ให้ ศชบ.ทอ.ปรับปรุงเนื้อหาตำราของหลักสูตรสายวิทยาการไซเบอร์จำนวน ๕ วิชา นั้น

๒. ศชบ.ทอ.ตรวจสอบและพิจารณาแก้ไขเนื้อหา รายละเอียดตามความเหมาะสม ร่วมกับ ร.อ.หญิง สุธิดา บทสันเทียะ นมฐ.ผมทส.กนผ.สนผ.ทสส.ทอ.แล้วเมื่อวันที่ ๒๓ ส.ค.๖๖ ดังมี รายละเอียดตามแนบ

จึงเสนอมาเพื่อพิจารณาดำเนินการให้ต่อไป

พล.อ.ต.
ผอ.ศชบ.ทอ.

กนผ.สนผ.ทสส.ทอ.
เลขรับ ๒๑๐๕
วันที่ ๒๘ ส.ค. ๖๖
เวลา ๑๓๕๗

ทราบแล้ว
- รอง ผอ.กนผ.สนผ.ทสส.ทอ.ทราบ
- ผสส.๑ ดำเนินการในส่วนที่เกี่ยวข้อง

น.อ.
ผอ.กนผ.สนผ.ทสส.ทอ.
๒๘ / ส.ค. / ๖๖

ทราบแล้ว

น.อ.
รอง ผอ.กนผ.สนผ.ทสส.ทอ.
๒๘ / ส.ค. / ๖๖

ทราบแล้ว

น.อ.
รอง ผอ.กนผ.สนผ.ทสส.ทอ.
๒๘ / ส.ค. / ๖๖

ระเบียบกองทัพอากาศ
ว่าด้วยการฝึกงานในหน้าที่
พ.ศ.๒๕๖๓

โดยที่เป็นการสมควรปรับปรุงแก้ไขแนวทางปฏิบัติเกี่ยวกับการฝึกงานในหน้าที่ของกองทัพอากาศ ให้เป็นไปด้วยความเรียบร้อย จึงวางระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า "ระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓"

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ให้ยกเลิก ระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๕๔

บรรดาระเบียบและคำสั่งอื่นใด ในส่วนที่กำหนดไว้แล้วในระเบียบนี้ หรือซึ่งขัดหรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน

ข้อ ๔ ในระเบียบนี้

๔.๑ "การฝึกงานในหน้าที่" หมายความว่า การให้นายทหารประทวนเข้ารับการฝึกงานตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย เพื่อเพิ่มพูนความรู้ ความสามารถ และความชำนาญให้สูงขึ้น ตามลักษณะความชำนาญทหารอากาศของเหล่าทหารหรือจำพวกทหาร โดยใช้ตามมาตรฐานการฝึกความชำนาญ และหนังสือคู่มือการฝึกงานในหน้าที่เป็นแนวทางการฝึก

๔.๒ "การฝึก" หมายความว่า การฝึกงานในหน้าที่

๔.๓ "นายทหารฝึกงานในหน้าที่" หมายความว่า นายทหารสัญญาบัตร ที่แต่งตั้งขึ้นให้มีหน้าที่รับผิดชอบ และดำเนินการ ควบคุม กำกับ ดูแล เกี่ยวกับการฝึกงานในหน้าที่ของหน่วยขึ้นตรงกองทัพอากาศ ให้ใช้คำย่อว่า "นฝน."

๔.๔ "ผู้ช่วยนายทหารฝึกงานในหน้าที่" หมายความว่า นายทหารสัญญาบัตรจำพวกทหารกำลังพลที่แต่งตั้งขึ้น ให้มีหน้าที่ช่วยเหลือนายทหารฝึกงานในหน้าที่ ให้ใช้คำย่อว่า "ผช.นฝน."

๔.๕ "เจ้าหน้าที่ฝึกงานในหน้าที่" หมายความว่า นายทหารสัญญาบัตร หรือนายทหารประทวน หรือลูกจ้างที่แต่งตั้งขึ้น ให้มีหน้าที่ด้านธุรการเกี่ยวกับการฝึกงานในหน้าที่ ให้ใช้คำย่อว่า "จนท.ฝน."

๔.๖ "ผู้ควบคุมการฝึก" หมายความว่า นายทหารสัญญาบัตรที่เป็นเหล่าหรือจำพวกทหารเดียวกันกับผู้รับการฝึกที่แต่งตั้งขึ้น ให้มีหน้าที่ดำเนินการ ควบคุม กำกับ ดูแลการฝึกงานในหน้าที่ภาคปฏิบัติประจำปีให้เป็นไปตามมาตรฐานการฝึกความชำนาญ

๔.๗ "ผู้ช่วยผู้ควบคุมการฝึก" หมายความว่า นายทหารสัญญาบัตรที่แต่งตั้งขึ้นให้มีหน้าที่ช่วยเหลือผู้ควบคุมการฝึก

๔.๘ "ครูฝึก"...

๓๑.๑๘.๒.๒ ระดับ ๕๐ จำนวนชั่วโมงรวมของการเรียนการสอนของภาคปฏิบัติและภาคบรรยาย ไม่เกินร้อยละ ๘๐ ของจำนวนชั่วโมงรวมในระดับ ๗๐

๓๑.๑๘.๒.๓ ระดับ ๗๐ จำนวนชั่วโมงรวมของการเรียนการสอนของภาคปฏิบัติและภาคบรรยาย ตรงกับความมุ่งหมายเฉพาะและวัตถุประสงค์การเรียนรู้ในระดับ ๗๐

๓๑.๑๙ หนังสือคู่มือการฝึกงานในหน้าที่ เป็นเอกสารอธิบายความรู้ในวิทยาการและวิธีปฏิบัติงานของเหล่าทหารหรือจำพวกทหารซึ่งส่วนราชการหัวหน้าสายวิทยาการจัดทำขึ้น เพื่อใช้ประกอบการฝึกงานในหน้าที่ตามระดับความชำนาญ โดยมีความสัมพันธ์และสอดคล้องกับเรื่องและหัวข้อวิชาในมาตรฐานการฝึกความชำนาญ ให้เรียกโดยย่อว่า "หนังสือคู่มือการฝึก" และให้จัดทำตามผนวก ๗ แนบท้ายระเบียบนี้

หมวด ๖
การควบคุมกำกับดูแล

ข้อ ๓๒ หน่วยฝึกจะต้องดำเนินการฝึกตามระยะเวลาที่กำหนดไว้ในวงรอบการฝึก

ข้อ ๓๓ ผู้รับการฝึก จะต้องทำการฝึกครบทุกหัวข้อวิชา หรือหมวดวิชาที่เป็นวิชาหลักของจำพวกทหารตามที่กำหนดในมาตรฐานการฝึกความชำนาญ

ข้อ ๓๔ เมื่อผู้รับการฝึกย้ายสังกัด ในระหว่างการฝึกภาคปฏิบัติ หรือรอการทดสอบภาควิชาการ ให้ส่วนราชการต้นสังกัดเดิมแจ้งให้ส่วนราชการต้นสังกัดใหม่ทราบถึงสถานภาพการฝึกที่ผ่านมา และเรื่องที่จะต้องดำเนินการต่อไป พร้อมกับส่งประวัติการฝึก กับมาตรฐานการฝึกความชำนาญไปยังส่วนราชการต้นสังกัดใหม่ โดยส่วนราชการต้นสังกัดใหม่จะต้องแต่งตั้งผู้รับผิดชอบในขั้นตอนที่ยังเหลืออยู่ เพื่อดำเนินการฝึกต่อไปให้ครบตามหัวข้อที่กำหนดไว้ หากจะให้ทำการฝึกที่ส่วนราชการเดิมต่อไป ให้ประสานตกลงกันแล้วแจ้งการเปลี่ยนแปลงให้ กรมกำลังพลทหารอากาศทราบ เพื่อแก้ไขเปลี่ยนแปลงหลักฐานการควบคุมการฝึกงานในหน้าที่ให้ถูกต้อง

ข้อ ๓๕ ผู้ที่ไม่สามารถทำการฝึกได้ครบตามที่กำหนด และอยู่ในกรณีที่จะต้องพ้นจากการฝึก ให้ส่วนราชการต้นสังกัดรายงานพร้อมหลักฐานประกอบให้กรมกำลังพลทหารอากาศ ดำเนินการนำเรียนขออนุมัติผู้บัญชาการทหารอากาศ หากจะเข้ารับการฝึกในปีต่อไปจะต้องเริ่มดำเนินการใหม่ ซึ่งการพ้นจากการฝึกจะต้องอยู่ในกรณี ดังนี้

๓๕.๑ ลาออก ให้ออก ปลดออก

๓๕.๒ ต้องหาคดีอาญา ยกเว้นความผิดลหุโทษ หรือความผิดตามกฎหมายอื่นที่มีอัตราโทษไม่สูงกว่าความผิดลหุโทษ

๓๕.๓ ย้าย โอน ไปสังกัดนอกกองทัพอากาศ

๓๕.๔ มีราชการจำเป็นเร่งด่วนและสำคัญ

๓๕.๕ มีเวลาการฝึกภาคปฏิบัติไม่ถึงร้อยละ ๘๕ ของเวลาการฝึกทั้งหมด โดยมีเหตุผลอันสมควร

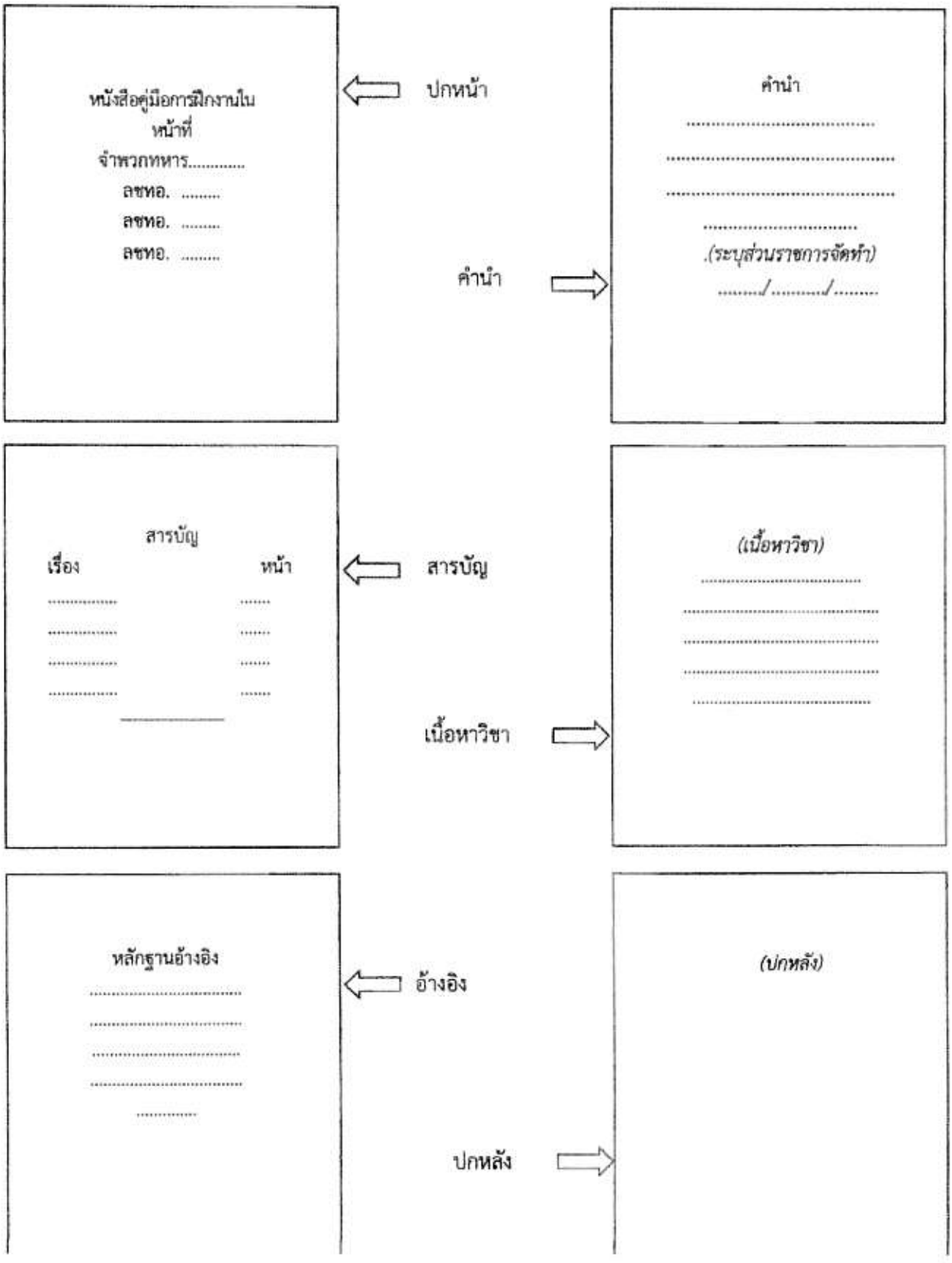
๓๕.๖ ป่วยจนมีเวลาการฝึกไม่เพียงพอตามข้อ ๓๕.๕

๓๕.๗ ขาดการทดสอบความรู้ภาคปฏิบัติตามระยะเวลาที่กำหนด โดยมีเหตุผลอันสมควร

ข้อ ๓๖ การลา ...

ผนวก ๗ ประกอบระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓

หนังสือคู่มือการฝึกงานในหน้าที่



คู่มือการฝึกงานในหน้าที่
จำพวกทหารไซเบอร์

ลชทอ.๒๘๑๓๐

ลชทอ.๒๘๑๕๐

ลชทอ.๒๘๑๗๐

กองรักษาความมั่นคงปลอดภัยไซเบอร์
ศูนย์ไซเบอร์กองทัพอากาศ

คำนำ

คู่มือการฝึกงานในหน้าที่วิชาการป้องกันทางไซเบอร์ จัดทำขึ้นเพื่อประกอบการฝึกความชำนาญตามมาตรฐานการฝึกความชำนาญ (มฝช.) ของสายวิทยาการไซเบอร์ เนื้อหาความรู้ของคู่มือเล่มนี้กล่าวถึงการป้องกันทางไซเบอร์ ได้แก่ ความหมาย หลักการ มาตรฐาน ขั้นตอน ระเบียบ เทคนิค อุปกรณ์การป้องกันทางไซเบอร์ และหน่วยงานที่เกี่ยวข้อง เพื่อให้ผู้เข้ารับการฝึกงานในหน้าที่มีความรู้ความเข้าใจและทักษะในการนำไปปฏิบัติงานในสายวิทยาการไซเบอร์ เกิดความปลอดภัยสูงสุดต่อผู้ปฏิบัติงาน ระบบคอมพิวเตอร์ และระบบสารสนเทศของกองทัพอากาศ

หวังเป็นอย่างยิ่งว่าคู่มือเล่มนี้ จะเป็นประโยชน์ต่อผู้เข้ารับการฝึกงานในหน้าที่และขอขอบคุณเจ้าหน้าที่ทุกท่านที่มีส่วนในการจัดทำคู่มือเล่มนี้จนเสร็จสมบูรณ์

กองรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ

๒๘ สิงหาคม ๒๕๖๖

สารบัญ

สารบัญภาพ

สารบัญภาพ (ต่อ)

บทที่ ๑ ความหมาย หลักการ และมาตรฐาน

ความพร้อมใช้งานของข้อมูลและระบบสารสนเทศต่าง ๆ ที่มีความจำเป็นในการใช้งานและเป็นไปตามกฎระเบียบและมาตรฐานที่กำหนดไว้ ซึ่งใช้มาตรการและเครื่องมือรักษาความปลอดภัยทางไซเบอร์เพื่อปกป้องข้อมูลที่ละเอียดอ่อนไม่ให้ถูกเข้าถึงโดยไม่ได้รับอนุญาต ตลอดจนป้องกันการหยุดชะงักของระบบสารสนเทศและโครงสร้างพื้นฐานทางสารสนเทศที่เป็นผลจากกิจกรรมในเครือข่ายที่ไม่พึงประสงค์ หน่วยงานที่รับผิดชอบจะต้องดำเนินการปรับใช้การรักษาความปลอดภัยทางไซเบอร์ โดยการปรับปรุงการป้องกันทางดิจิทัลระหว่างเครือข่ายและบุคลากรของ ทอ. กระบวนการ และเทคโนโลยีต่าง ๆ ให้ทันยุคสมัยและเหมาะสมกับสถานการณ์

๑.๑ ความหมายของการป้องกันทางไซเบอร์

การป้องกันทางไซเบอร์ หมายถึง กระบวนการที่เป็นการรักษาความมั่นคงปลอดภัยทางไซเบอร์ คือแนวปฏิบัติในการปกป้องคอมพิวเตอร์ เครือข่าย ซอฟต์แวร์ แอปพลิเคชัน ระบบที่สำคัญ และข้อมูล จากภัยคุกคามทางดิจิทัลที่อาจเกิดขึ้นได้ โดยจะต้องมีองค์กรหรือหน่วยงานที่มีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยข้อมูลหรือระบบสารสนเทศรวมไปถึงเครือข่ายทั้งภายในและภายนอก ทอ. เพื่อรักษาความถูกต้องของข้อมูล ความลับของข้อมูลหรือสิทธิ์การเข้าใช้งานสำหรับผู้ที่ได้รับอนุญาตเท่านั้น

๑.๒ หลักการพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศ

หลักการพื้นฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ คือ การสร้างความมั่นใจในการรักษาความลับ ความถูกต้องสมบูรณ์ และสภาพความพร้อมใช้ของ สารสนเทศ ตลอดจนข้อมูล ระบบสารสนเทศ และทรัพย์สินสารสนเทศ ซึ่งครอบคลุมถึงข้อมูลที่จัดเก็บ ประมวลผล และรับส่งผ่านเครือข่าย จากการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานโดยไม่ได้รับอนุญาต การใช้ในทางที่ผิด การทำลายหรือการเปลี่ยนแปลง โดยมีการบริหาร จัดการความเสี่ยง และนำมาตรการต่าง ๆ ด้านบริหารจัดการ ด้านเทคนิค ด้านกายภาพที่เหมาะสมมาใช้จัดการภัยคุกคามต่าง ๆ ซึ่งประกอบด้วยส่วนที่สำคัญ ๔ ด้าน คือ

๑.๒.๑ ความรู้พื้นฐานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยให้กับข้อมูล สารสนเทศ และระบบสารสนเทศ องค์ประกอบคุณสมบัติหลักด้านความมั่นคงปลอดภัยสารสนเทศ ๓ ด้าน (การรักษาความลับ ความถูกต้อง และความพร้อมใช้) และองค์ประกอบสำคัญอื่นที่เกี่ยวข้อง แนวคิดความสัมพันธ์ของสามเหลี่ยมด้านความมั่นคงปลอดภัย ฟังก์ชันการทำงาน และ การใช้งาน (The Security, Functionality and Usability Triangle) สำหรับการกำหนดระดับความมั่นคงปลอดภัยสารสนเทศ รูปแบบการโจมตีด้านความมั่นคงปลอดภัยสารสนเทศ ประเภท ภัยคุกคามและช่องโหว่ ลักษณะภัยคุกคามทางไซเบอร์ แนวโน้มด้านความมั่นคงปลอดภัย การบริหาร ความเสี่ยงและมาตรการจัดการความเสี่ยง

๑.๒.๒ Data Security คือ หลักการหรือเทคโนโลยีที่ช่วยในการปกป้องข้อมูลจากการทำลาย แก้ไข หรือเปิดเผยข้อมูลทั้งเจตนาและไม่เจตนา โดยการนำเทคนิคต่าง ๆ และเทคโนโลยีที่หลากหลายมาควบคุมและจัดการความปลอดภัย เป้าหมายหลักของการรักษาความปลอดภัยข้อมูลคือการปกป้องข้อมูลที่องค์กรรวบรวม เก็บ สร้าง รับ หรือส่ง ไม่สำคัญว่าจะต้องใช้อุปกรณ์เทคโนโลยีหรือกระบวนการใดในการจัดการแต่จะต้องได้รับการปกป้อง การฝ่าฝืนข้อมูลอาจส่งผลให้เกิดคดีฟ้องร้อง ค่าปรับจำนวนมาก และส่งผลเสียต่อชื่อเสียงขององค์กร ความสำคัญของการป้องกันข้อมูลจากภัยคุกคามด้านความปลอดภัยจึงมีความสำคัญมากในปัจจุบัน

๑.๒.๓ Confidentiality Integrity และ Availability (CIA Triad)

๑.๒.๓.๑ Confidentiality หมายถึง ความสามารถในการรักษาความลับของระบบการควบคุมการเข้าถึงข้อมูลเพื่อไม่ให้ผู้ที่ไม่มีสิทธิ์เข้าถึงความลับใด ๆ เช่น หากเรามีการเก็บข้อมูลส่วนบุคคลไว้ ได้แก่ เลขบัตรประชาชน เบอร์โทร โรคประจำตัว หน้าที่ของระบบคือการจัดการความปลอดภัยไม่ให้คนที่ไม่มีสิทธิ์เข้ามาดูข้อมูลของเราไปได้ เป็นต้น

๑.๒.๓.๒ Integrity หมายถึง ความถูกต้องและความสมบูรณ์ของข้อมูลไม่ว่าจะเป็นการส่งหรือจัดเก็บ เช่น หากเราส่งข้อมูลจากจุด A ไปจุด B หรือ B จัดเก็บข้อมูลไว้ ข้อมูลนั้นควรถูกต้องสมบูรณ์เสมอจากต้นฉบับ (A) หรือจะเปลี่ยนแปลงแก้ไขได้จากผู้ที่ได้รับสิทธิ์เท่านั้น หน้าที่ของระบบคือป้องกันการโจมตี แก้ไขหรือเปลี่ยนแปลงข้อมูลโดยผู้ที่ไม่มีสิทธิ์

๑.๒.๓.๓ Availability หมายถึง ความสามารถของระบบที่จะคงอยู่ ให้บริการหรือทำงานได้ตลอดเวลาจากคนที่มีสิทธิ์ หน้าที่ของระบบคือแม้จะเกิดข้อผิดพลาดใด ๆ ต้องมีมาตรการสำรองเตรียมพร้อมไว้เสมอ เพื่อให้ระบบยังคงดำเนินการได้ ยังมีอีกคุณสมบัติที่สำคัญ ไม่น้อยไปกว่า CIA Triad นั้นก็คือ AAA protocol

ภาพที่ ๑ แนวคิด ๓ เสาหลักในด้านความมั่นคงปลอดภัยสารสนเทศ

๑.๒.๔ AAA Protocol คือ Protocol ที่มี ๓ องค์ประกอบ ได้แก่

๑.๒.๔.๑ Authentication คือ การตรวจสอบและพิสูจน์ตัวตน เพื่อเข้าใช้งานระบบ ซึ่งมีหลายวิธีไม่ว่าจะเป็น User & Password, PIN, QR code ลายนิ้วมือหรือใบหน้า

๑.๒.๔.๒ Authorization คือ การกำหนดสิทธิ์การเข้าถึงให้แก่บุคคลว่าบุคคลไหนสามารถใช้งานอะไรในระบบได้บ้าง เช่น บางคนอาจจะสามารถดูข้อมูลในไฟล์ได้แต่จะไม่สามารถแก้ไขได้ เป็นต้น

๑.๒.๔.๓ Accounting คือ กระบวนการเก็บและบันทึกว่าแต่ละคนเข้ามาเปลี่ยนแปลงแก้ไขอะไรบ้าง เพื่อเก็บข้อมูลไว้ตรวจสอบหรือใช้ในการร่าง Policy ได้

จากที่กล่าวมาแล้วนั้น ทั้ง CIA Triad และ AAA protocol เป็นคุณสมบัติที่สำคัญอย่างยิ่งในการรักษาความปลอดภัยและสร้างความน่าเชื่อถือให้แก่ตัวระบบ โดยที่ระบบต้อง รักษาความลับ รักษาข้อมูลให้ถูกต้องและพร้อมใช้งานอยู่เสมอ รวมถึงคนที่มีสิทธิ์ต้องยืนยันตัวตนเพื่อเข้าใช้งาน และมีการกำหนดสิทธิ์ของผู้ใช้แต่ละคนโดยต้องมีการเก็บข้อมูลประวัติการใช้งานหรือการเพิ่ม ลบ เปลี่ยนแปลงข้อมูลได้ด้วย

ภาพที่ ๒ คุณสมบัติที่สำคัญในการรักษาความปลอดภัยสารสนเทศ (AAA protocol)

๑.๓ มาตรฐานการรักษาความปลอดภัย

การรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นการปกป้องด้านความมั่นคงปลอดภัย จากภัยคุกคามต่าง ๆ ตามเป้าหมายของการรักษาความมั่นคงปลอดภัยสารสนเทศ ในการรักษาความลับ ความถูกต้องสมบูรณ์ และสภาพความพร้อมใช้ สำหรับ ข้อมูล สารสนเทศ และระบบสารสนเทศ ในสภาพแวดล้อมไซเบอร์ ที่มีการให้บริการ หรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่าย ที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป ทั้งนี้ เพื่อดำเนินการมาตรการจัดการภัยคุกคามทางไซเบอร์ โดยมีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) จะต้องมีการประเมินและตรวจสอบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือคาดว่าจะเกิดขึ้นหรือไม่ โดยให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

๑.๓.๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework)

๑.๓.๑.๑ NIST Cybersecurity Framework

จุดเริ่มต้นของมาตรฐานเกิดขึ้นจากรัฐบาลของประเทศสหรัฐอเมริกา ได้มอบหมายให้สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) พัฒนากรอบการดำเนินงานเพื่อปรับปรุงความมั่นคงปลอดภัยไซเบอร์ ของหน่วยงานระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) เพื่อให้เป็นแนวทางและมาตรฐาน ซึ่งครอบคลุมทั้งในระดับนโยบาย การจัดการองค์กร และเทคโนโลยี เพื่อบริหารความเสี่ยงไซเบอร์ที่มีผลกระทบกับหน่วยงานโครงสร้างพื้นฐานสำคัญได้อย่างเหมาะสม

๑.๓.๑.๒ NIST Cybersecurity Framework Version 1.1 (ปรับปรุงเมื่อ เม.ย.๒๕๖๑) เป็นกรอบการดำเนินงานที่ประกอบด้วย ๓ องค์ประกอบหลักที่เรียกว่า Framework Core, Framework Implementation Tiers และ Framework Profiles เพื่อกำหนดแนวปฏิบัติที่ดี และนำไปใช้ในการจัดการระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII)

๑.๓.๒ องค์ประกอบ Framework Core Functions แบ่งย่อยออกเป็นกิจกรรมงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ได้อย่างเหมาะสม โดยการกำหนดผลลัพธ์ที่ต้องการและกรอบปฏิบัติที่อ้างอิงสำหรับการดำเนินงานเพื่อบรรลุตามวัตถุประสงค์ของแต่ละอุตสาหกรรมโครงสร้างพื้นฐาน จะช่วยให้องค์กรเข้าใจ และ จัดทำโครงงานและระบบด้าน Cybersecurity ได้อย่างมีประสิทธิภาพมากขึ้นโดยหัวใจสำคัญของ Framework แบ่งออกเป็น ๕ ฟังก์ชันหลัก ได้แก่

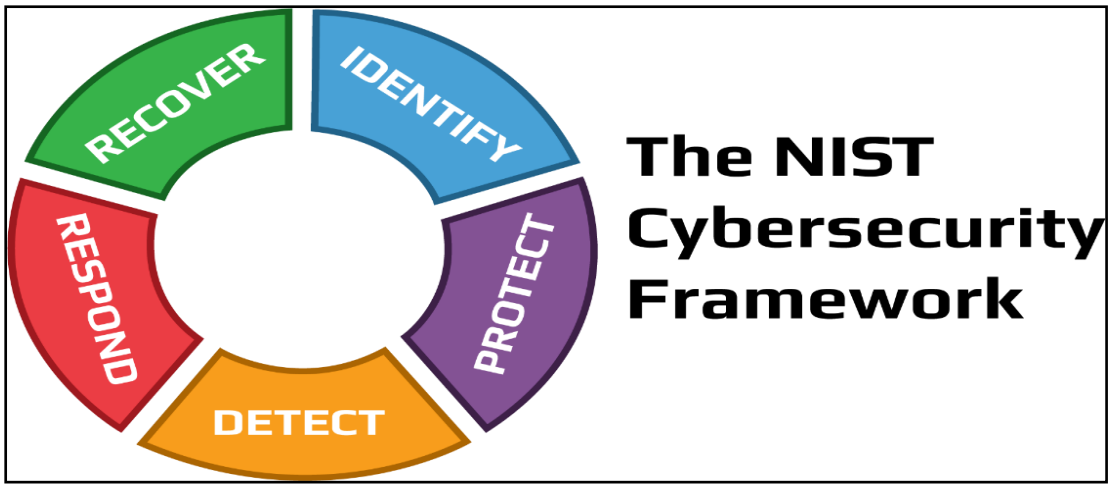
๑.๓.๒.๑ การระบุ (Identify) เป็นขั้นตอนแรกในการศึกษาทำความเข้าใจบริบท ทรัพยากร และกิจกรรมงานสำคัญ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูล และขีดความสามารถ

๑.๓.๒.๒ การป้องกัน (Protect) เป็นการจัดทำและดำเนินการตามมาตรการป้องกันที่เหมาะสมสำหรับการให้บริการโครงสร้างพื้นฐานสำคัญ โดยมีวัตถุประสงค์เพื่อจำกัดระดับผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ครอบคลุมการฝึกอบรมและการสร้างความตระหนักถึงมาตรการควบคุมการเข้าถึง และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี

๑.๓.๒.๓ การตรวจจับ (Detect) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวังหรือตรวจติดตามต่อเนื่อง

๑.๓.๒.๔ การตอบสนอง (Respond) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุง

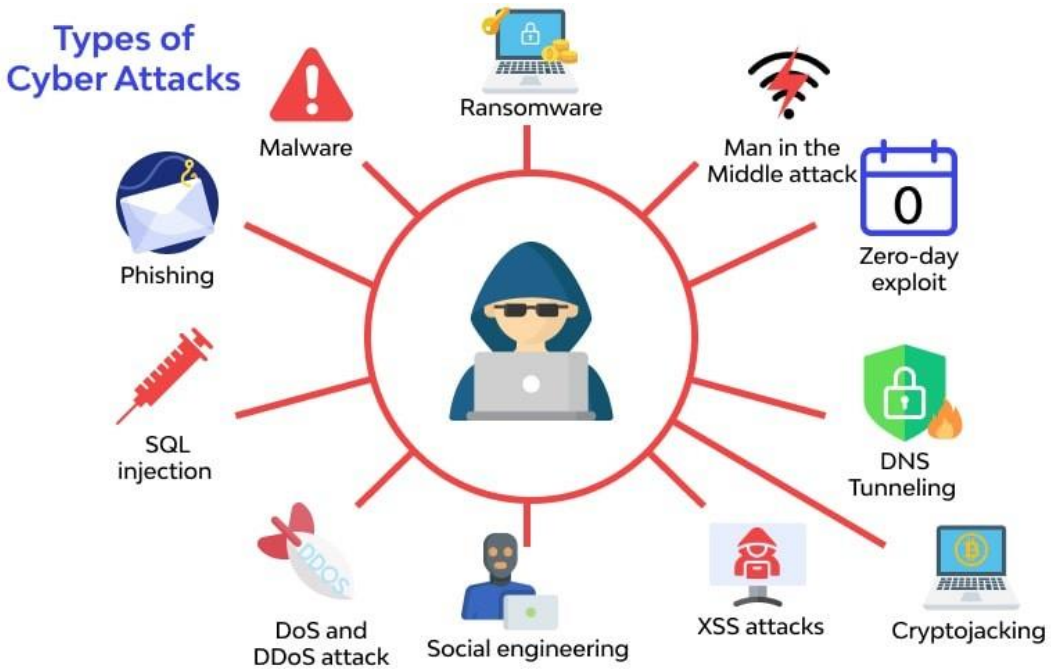
๑.๓.๒.๕ การคืนสภาพ (Recover) เป็นการจัดทำและดำเนินกิจกรรมตามแผนงานเพื่อรองรับการดำเนินงานต่อเนื่อง รวมถึงแผนการกู้คืนทั้งด้านขีดความสามารถและบริการให้ได้ตามที่กำหนด



ภาพที่ ๓ กรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (NIST Framework)

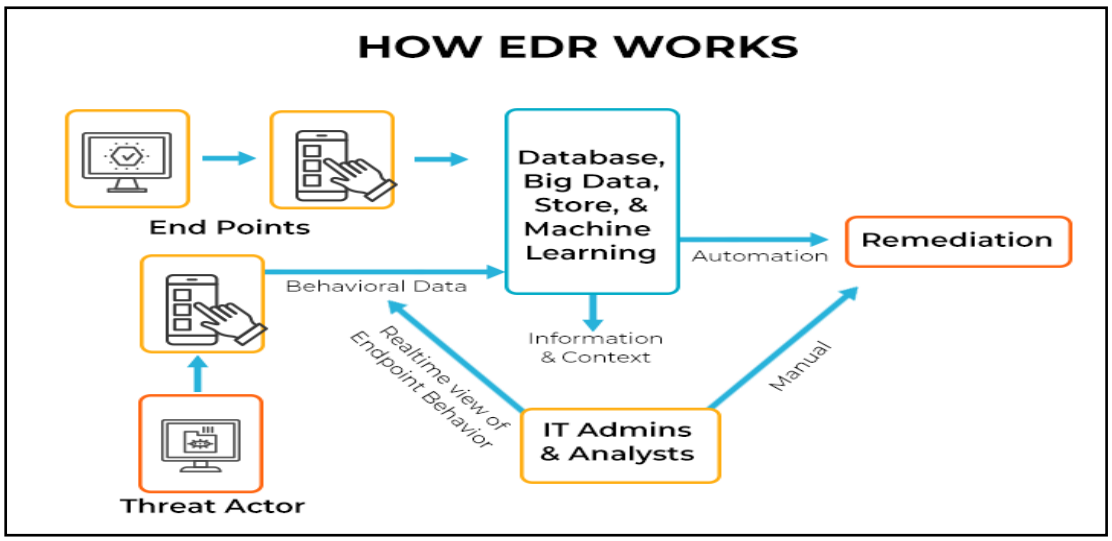
๑.๓.๓ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ ประกอบด้วยการป้องกัน ๓ ส่วนที่สำคัญ ดังนี้

๑.๓.๓.๑ การป้องกันเครื่องลูกข่าย (Host-Based Protection) จากสถานการณ์การโจมตีในปัจจุบันมีการใช้งานอุปกรณ์คอมพิวเตอร์ในการทำงานกันอย่างแพร่หลาย จึงปฏิเสธไม่ได้เลยว่าคอมพิวเตอร์คืออุปกรณ์หลักในการดำเนินการหรือดำเนินกิจกรรมต่าง ๆ และเมื่อมีการใช้งานจำนวนมากย่อมเป็นเป้าหมายในการโจมตีทางไซเบอร์มากขึ้นตามมาด้วย โดยมีการสร้างหรือพัฒนาเครื่องมือและเทคนิคต่าง ๆ เพื่อจะโจมตีทางไซเบอร์กับเครื่องผู้ใช้งานโดยใช้มัลแวร์ชนิดต่าง ๆ ในการโจมตีทางไซเบอร์ ซึ่ง Malicious และ Software หมายถึง โปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้น เพื่อทำอันตรายกับระบบคอมพิวเตอร์ เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติ ขโมยหรือทำลายข้อมูลหรืออาจจะเปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่องของเราได้ ดังนั้นจึงต้องมีการป้องกันเครื่องผู้ใช้งานที่เชื่อมต่อกับเครือข่ายทั้งภายในและภายนอก เพราะเครื่องคอมพิวเตอร์จะถูกนำไปใช้เป็นเครื่องมือในการโจมตีทางไซเบอร์ภายในองค์กร และยังสามารถใช้เป็นเครื่องเหยื่อและฐานในการโจมตีไปยังภายนอกองค์กรได้



ภาพที่ ๔ ภัยคุกคามทางไซเบอร์ที่โจมตีเครื่องคอมพิวเตอร์

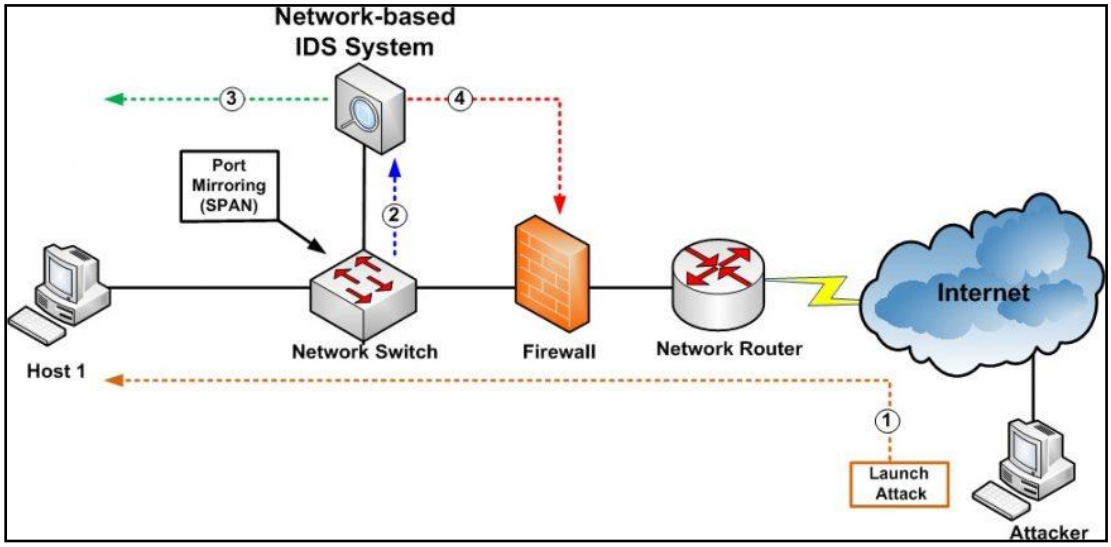
การป้องกันเครื่องลูกข่ายภายใน ทอ. ในปัจจุบันมีการแนะนำให้ติดตั้งโปรแกรมป้องกัน มัลแวร์บนเครื่องคอมพิวเตอร์ที่ไม่ใช้งานด้านการยุทธของ ทอ. เช่น โปรแกรม Avast และ Bitdefender เป็นต้น ส่วนการป้องกันเครื่องคอมพิวเตอร์ที่ใช้ในงานสำคัญและด้านการยุทธของ ทอ. มีนโยบายให้ติดตั้งโปรแกรมป้องกันมัลแวร์ชนิด Endpoint Detection and Response (EDR) ซึ่งจะมีสมรรถนะสูงกว่าโปรแกรมป้องกันมัลแวร์ทั่วไป เนื่องจากมีการใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) มาวิเคราะห์พฤติกรรมของผู้ใช้งานด้วย ทำให้สามารถป้องกันมัลแวร์ได้ดียิ่งกว่าเดิม โดย ทอ.มีการใช้งานโปรแกรมป้องกันมัลแวร์ที่ชื่อว่า Deep Instinct ซึ่งจะมีการแจ้งเตือนหรือมีการสรุปผลการทำงานของโปรแกรมมายังผู้รับผิดชอบในการเฝ้าระวังป้องกันทางไซเบอร์ให้ดำเนินการตรวจสอบได้



ภาพที่ ๕ หลักการทำงานของโปรแกรมป้องกันมัลแวร์ชนิด Endpoint Detection and Response (EDR)

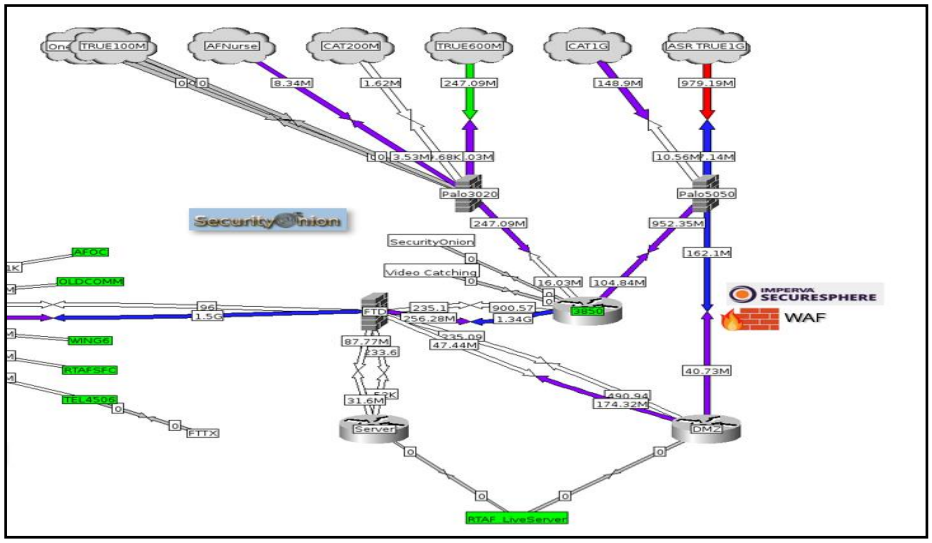
๑.๓.๓.๒ การป้องกันเครือข่ายกองทัพอากาศ (Network-Based Protection)

ในปัจจุบันมีการทำงานเชื่อมโยงกันระหว่างคอมพิวเตอร์หลายเครื่องภายในองค์กรเพื่อดำเนินการต่าง ๆ อย่างมากมาย จึงมีการใช้งานเครือข่ายอินทราเน็ตและอินเทอร์เน็ตกันเป็นจำนวนมาก ดังนั้นการป้องกันเครือข่ายภายในให้ปลอดภัยจากภัยคุกคามจากภายนอกที่มีความพยายามโจมตีเข้ามายังเครื่องเครือข่ายภายใน โดยถึงแม้จะไม่สามารถดำเนินการยึดหรือควบคุมแต่อาจสามารถแสวงหาผลประโยชน์ได้จากการทำสำเนาข้อมูลที่ทำการติดต่อสื่อสารกันระหว่างเครื่อง ทำให้เกิดการสูญเสียข้อมูล หรือการดักจับข้อมูลที่เป็นความลับ ซึ่งทำให้หลักการให้การรักษาความลับบกพร่องไป เครือข่ายจึงเป็นสิ่งที่จำเป็นในการป้องการโจมตีทางไซเบอร์อย่างยิ่ง เนื่องจากสามารถกำหนดและตั้งค่าการติดต่อสื่อสารให้เป็นไปตามนโยบายขององค์กรได้ เช่น การอนุญาตให้ติดต่อกับไอพีปลายทางใด และการปิดกั้นการเชื่อมต่อไปยังไอพีปลายทาง เป็นต้น



ภาพที่ ๖ ผังการทำงานของระบบป้องกันเครือข่าย (Network-Based Protection)

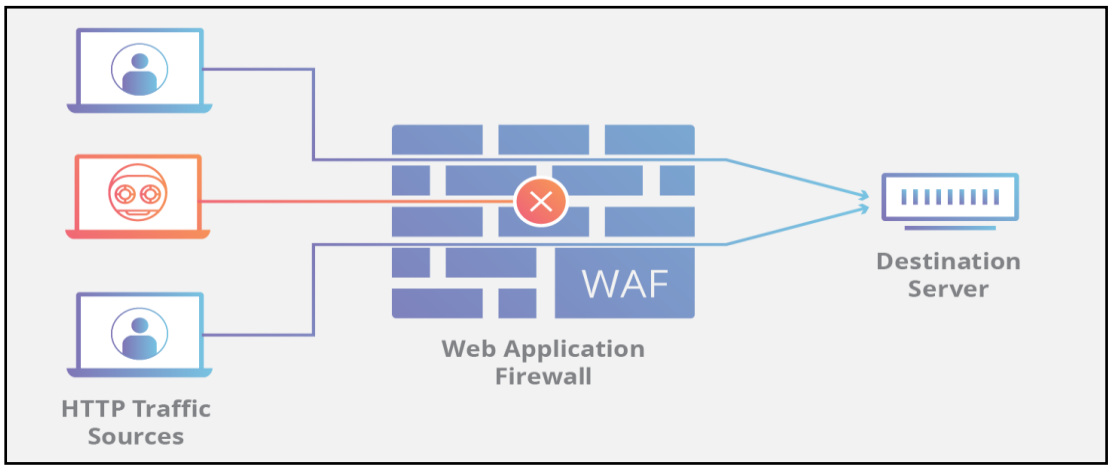
โดยการป้องกันเครือข่ายของ ทอ. นั้น จะมีหลายระบบและหลายอุปกรณ์ในการเฝ้าระวัง และป้องกันภัยคุกคามทางไซเบอร์ ไม่ว่าจะเป็นระบบป้องกันเครือข่าย (Firewall) ระบบแจ้งเตือนการบุกรุก (IDS) โดยจะได้กล่าวถึงในบทถัดไป ดังนั้นการป้องกันเครือข่ายจึงเป็นสิ่งที่สำคัญอย่างยิ่งสำหรับองค์กรขนาดใหญ่ที่มีการเชื่อมโยงข้อมูลจำนวนมหาศาล โดยจะต้องมีหน่วยงานในการกำกับ ดูแลรับผิดชอบในการบำรุงรักษาระบบงานหรืออุปกรณ์ในการป้องกันเครือข่ายให้สามารถป้องกันได้อย่างต่อเนื่องและมีประสิทธิภาพ และต้องมีหน่วยงานที่กำหนดนโยบายในการใช้งานเครือข่ายเพื่อควบคุมการเชื่อมต่อให้ปลอดภัย รวมไปถึงจะต้องมีหน่วยงานที่เฝ้าระวังและตรวจสอบข้อมูลจากระบบเหล่านั้นเพื่อให้มั่นใจได้ว่าระบบงานหรือข้อมูลขององค์กรปลอดภัย และเครื่องคอมพิวเตอร์ขององค์กรจะปลอดภัยจากภัยคุกคามทางไซเบอร์



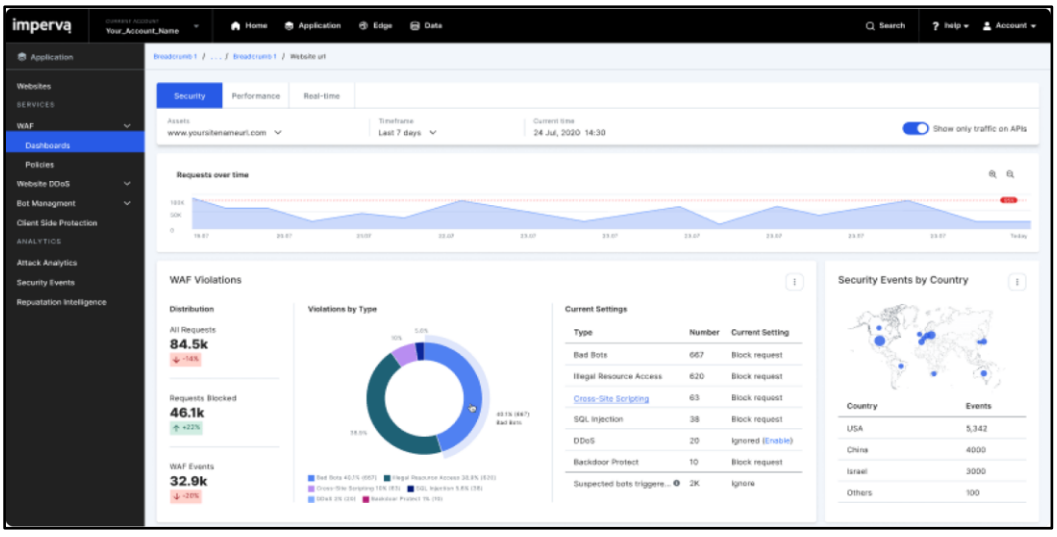
ภาพที่ ๗ แผนผังตัวอย่างการวางระบบป้องกันเครือข่าย ทอ.

๑.๓.๓.๓ การป้องกันเว็บไซต์ภายใต้โดเมนกองทัพอากาศ (Web Protection)

องค์กรในปัจจุบันไม่ว่าจะเป็นภาครัฐและเอกชนมีการประชาสัมพันธ์หน่วยงานหรือมีการใช้งานระบบออนไลน์ จึงปฏิเสธไม่ได้เลยว่าทุกองค์กรจะต้องมีเว็บไซต์ และแนวโน้มจะมีการใช้งานเว็บไซต์มากยิ่งขึ้น เนื่องจากสามารถลดค่าใช้จ่ายและลดเวลาปฏิบัติงานรวมถึงสามารถเข้าถึงการใช้งานได้จากระยะไกลผ่านเทคโนโลยีเว็บไซต์ แต่เมื่อใดก็ตามที่มีผู้นิยมใช้ก็เป็นช่องทางที่ทำให้ผู้ไม่หวังดีเข้ามาแสวงหาผลประโยชน์เสมอ ดังนั้นจึงจำเป็นต้องมีการเฝ้าระวังและป้องกันเว็บไซต์ให้ปลอดภัยจากภัยคุกคามทางไซเบอร์เพื่อรักษาความพร้อมใช้งาน บางครั้งอาจเป็นเพราะรักษาความน่าเชื่อถือขององค์กรได้ ซึ่งหากเว็บไซต์ประชาสัมพันธ์มีการถูกโจมตีหรือเปลี่ยนแปลงหน้าเว็บไซต์จะถูกลดทอนความน่าเชื่อถึงขององค์กรเป็นอย่างมาก จึงมีความจำเป็นอย่างยิ่งในการป้องกัน การโจมตีเว็บไซต์

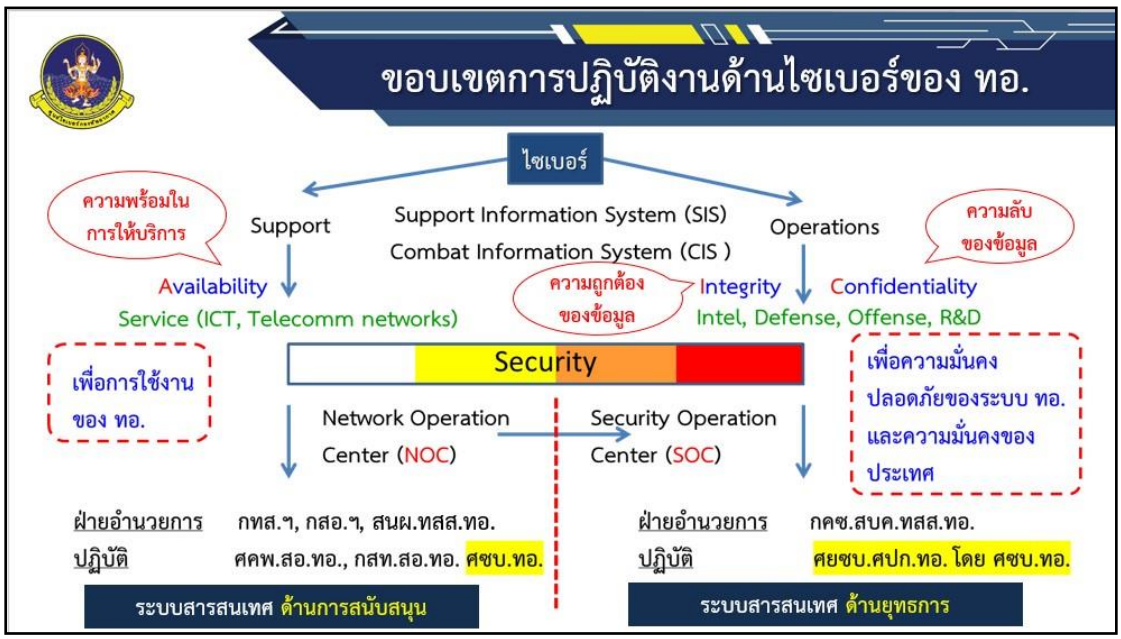


ภาพที่ ๘ ผังการทำงานของระบบการป้องกันเว็บไซต์ (Web Protection)



ภาพที่ ๙ ตัวอย่างระบบ Imperva เป็นการป้องกันเว็บไซต์ (Web Application Firewall)

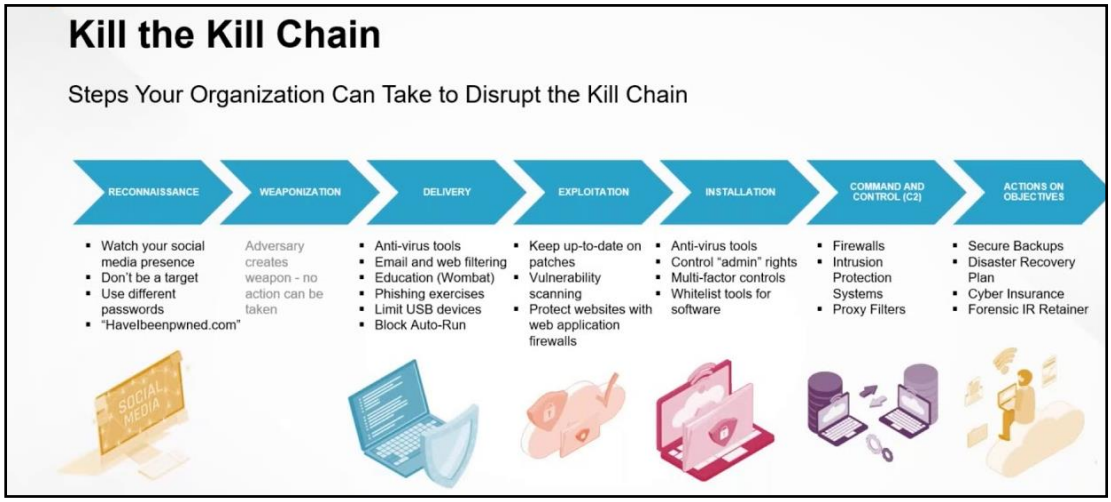
การป้องกันเว็บไซต์สามารถทำได้หลายวิธีโดยสามารถใช้งานระบบหรือโปรแกรมป้องกันการโจมตีเว็บไซต์ซึ่งมีทั้งแบบมีค่าใช้จ่ายและไม่เสียค่าใช้จ่าย ทั้งนี้ระบบป้องกันเว็บไซต์ที่ดีจะต้องมีการอัปเดตฐานข้อมูลการโจมตีในรูปแบบใหม่ ๆ ได้ โดยจะมีองค์กรหลายองค์กรที่จัดทำหรือรวบรวมวิธีการต่าง ๆ ในการโจมตีทางไซเบอร์ไว้ และในหมวดหมู่ของการโจมตีเว็บไซต์มีแยกประเภทการโจมตี โดยในปัจจุบัน ทอ. มีการใช้งานระบบป้องกันเว็บไซต์ภายใต้โดเมนกองทัพอากาศ (RTAF Web Protection) ชื่อ Imperva ซึ่งเป็นระบบงาน เกี่ยวกับการป้องกันเว็บไซต์ (Web Application Firewall) อีกทั้งยังมีโครงการวิจัยและพัฒนา Mod Security (Open Source) เพื่อเป็นทางเลือกในการป้องกันเว็บไซต์ภายใต้โดเมน ทอ.สำหรับการปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ทอ.จัดให้มีการดำเนินการตลอด ๒๔ ชั่วโมงตลอด ๗ วันต่อสัปดาห์ ทั้งนี้ยังรวมถึงผู้ที่เกี่ยวข้องกับงานด้านเทคโนโลยีสารสนเทศของ ทอ. อีกด้วย โดยการปฏิบัติการเฝ้าระวังทางไซเบอร์ของ ทอ.นั้นจะมีการจัดตั้งศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ที่นิยมเรียกกันว่า CSOC โดยย่อมาจากคำว่า Cybersecurity Operation Center มีหน้ารับผิดชอบในการเฝ้าระวังและตรวจจับภัยคุกคามหรือการโจมตีระบบสารสนเทศและการสื่อสารของ ทอ.



ภาพที่ ๑๐ ขอบเขตการปฏิบัติงานด้านไซเบอร์ของ ทอ.

๑.๓.๔ กระบวนการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ

หลักคิดในการป้องกันเครื่องผู้ใช้งาน เครือข่ายภายใน และระบบสารสนเทศต่าง ๆ ของ ทอ. เกิดขึ้นจากกระบวนการโจมตีหรือคุกคามทางไซเบอร์ในรูปแบบของการเจาะระบบเพื่อโจมตีทางไซเบอร์ (Cyber Kill Chain) ที่มี ๗ ขั้นตอนนั้นเป็นโมเดลในการออกแบบการป้องกัน เนื่องจากการที่เราจะป้องกัน ผู้ไม่หวังดีหรือแฮ็กเกอร์ได้นั้นมีความจำเป็นต้องเข้าใจการดำเนินการโจมตีของผู้ไม่หวังดีก่อน แล้วจึงนำกระบวนเหล่านั้นมาวิเคราะห์เพื่อหาจุดที่จะดำเนินการป้องกันให้เหมาะสมกับกองทัพอากาศ เนื่องจากต้องคำนึงถึงผลกระทบที่จะเกิดขึ้น ด้วยงบประมาณที่จำกัด และจำนวนบุคลากรที่มีองค์ความรู้ ด้านไซเบอร์ ควบคู่ไปกับการเผยแพร่องค์ความรู้ด้านความมั่นคงปลอดไซเบอร์ไปยังบุคลากรด้านอื่น ๆ ของ ทอ. ให้ครบถ้วน ในปัจจุบันปฏิเสธไม่ได้เลยว่า มนุษย์คือจุดอ่อนของระบบสารสนเทศโดยแท้จริง ผู้ไม่หวังดีหรือแฮ็กเกอร์จึงมีการโจมตีหรือคุกคามไปยังบุคลากรก่อนเป็นอันดับแรก ทำให้การให้ความรู้จึงเป็นสิ่งที่สำคัญ



ภาพที่ ๑๑ การเจาะระบบเพื่อโจมตีทางไซเบอร์ (Cyber Kill Chain)

เมื่อได้ศึกษาแนวทางในการเจาะระบบเพื่อโจมตีทางไซเบอร์ (Cyber Kill Chain) แล้วนั้นจะพบว่ากระบวนการที่เหมาะสมและคุ้มค่าที่จะดำเนินการมากที่สุดคือ การตัดวงจรไม่ให้ผู้ไม่หวังดีหรือแฮ็กเกอร์ทำตามเป้าหมายที่วางแผนได้ ในขั้นตอนที่ ๖ คือการควบคุมและสั่งการจากผู้ไม่หวังดี (Command and Control) ซึ่งมีความเสี่ยงสูงในการที่อาจจะทำให้ระบบสารสนเทศต่าง ๆ ของ ทอ. ไม่ปลอดภัย หากถูกควบคุมและสั่งการจากระยะไกลเพื่อใช้เป็นฐานในการโจมตีไปยังภายในและภายนอกเครือข่าย ทอ.

ภาพที่ ๑๒ การเจาะระบบเพื่อโจมตีทางไซเบอร์ (Cyber Kill Chain)

จากภาพที่ ๑๒ จะเห็นได้ว่าความเสี่ยงยิ่งสูงมากเพียงใดค่าใช้จ่ายหรือทรัพยากรในการรักษาความมั่นคงปลอดภัยทางไซเบอร์น้อยลงตามไป ด้วยงบประมาณที่จำกัดการปิดกั้นการเชื่อมต่อเพื่อป้องกันไม่ให้เครื่องลูกข่ายภายใน ทอ. ทำการติดต่อสื่อสารไปยังไอพีปลายที่ของผู้ไม่หวังดีได้จึงเป็นวิธีการที่เหมาะสมที่สุดในปัจจุบัน ซึ่งการดำเนินการปิดกั้นสามารถทำได้ง่ายและหลากหลายวิธีการ แต่หนึ่งวิธีการที่นิยมและเห็นผลมากที่สุด คือการใช้งานหรือการตั้งค่าอุปกรณ์ป้องกันเครือข่าย (Firewall) และอาจจะมีการใช้งานระบบอื่น ๆ เข้ามาทำงานประสานกันได้เพื่อให้ได้ประสิทธิภาพในการเฝ้าระวังป้องกันสูงสุดเท่าที่งบประมาณจะสามารถดำเนินการได้

ภาพที่ ๑๓ การปิดกั้นไอพีที่เป็นภัยคุกคามด้วยระบบป้องกันเครือข่ายโดยระบบ Palo Alto (Next Gen Firewall)

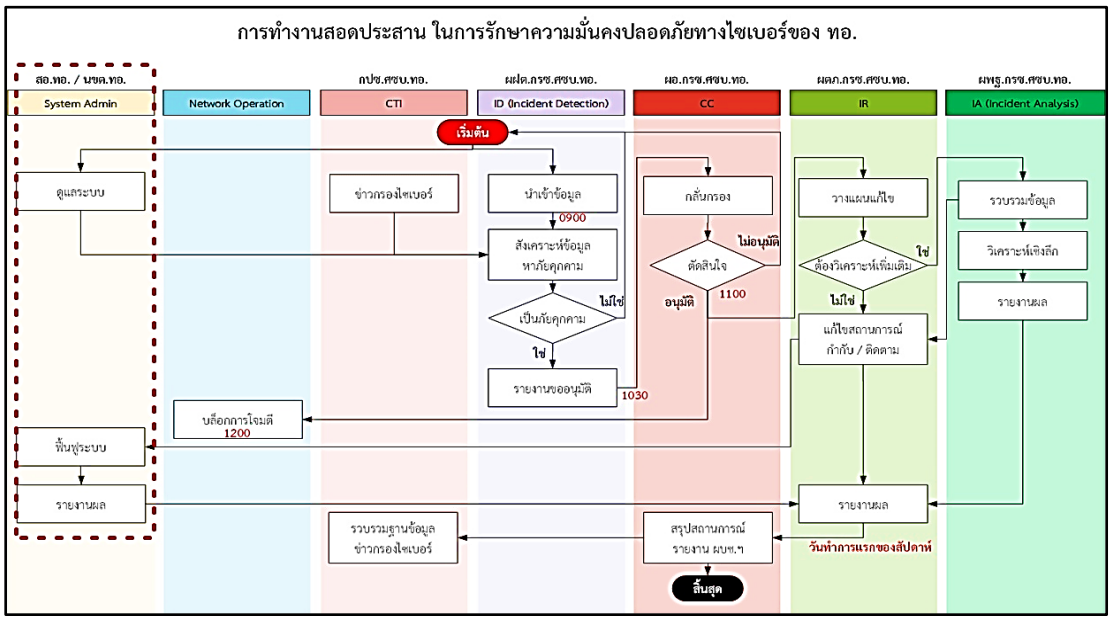
บทที่ ๒ ขั้นตอน แผนการปฏิบัติ และระเบียบ

การรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้มีประสิทธิภาพ เป็นระบบและปฏิบัติการตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว มีความจำเป็นต้องนำข้อมูลต่าง ๆ มาผ่านกระบวนการวิเคราะห์และการตัดสินใจ เพื่อนำไปพิจารณากำหนดเป็นแนวทางในการปฏิบัติ โดยการปฏิบัตินั้นต้องอยู่ภายใต้ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัย ระบบสารสนเทศ พ.ศ.๒๕๖๓ โดยมีรายละเอียด ดังนี้

๒.๑ ขั้นตอนการปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ ทอ.

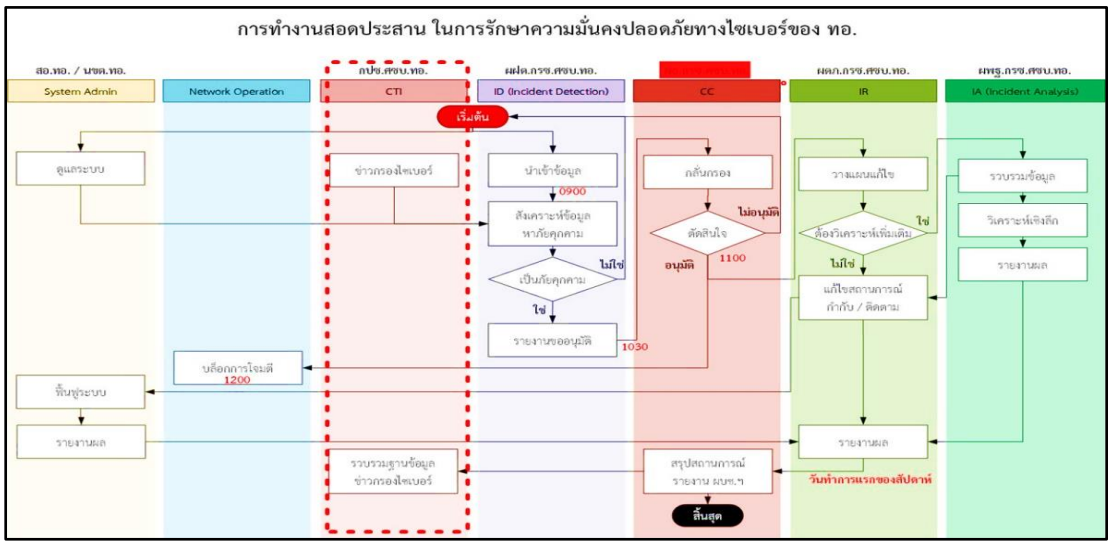
ยึดหลักการทำงานที่สอดประสานการปฏิบัติเมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ เพื่อการตอบสนองภัยคุกคามได้อย่างเหมาะสมตามกรอบและวงรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของ NIST โดยมีองค์ประกอบ ดังนี้

๒.๑.๑ ขั้นตอนส่วนของผู้ดูแลระบบ ได้แก่ สอ.ทอ./นขต.ทอ. มีหน้าที่รายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ ฟื้นฟูระบบ และตอบสนอง ซึ่งจะรายงานต่อ ชุดเฝ้าระวังทางไซเบอร์ ศูนย์ยุทธการทางไซเบอร์ ศูนย์ปฏิบัติการกองทัพอากาศ



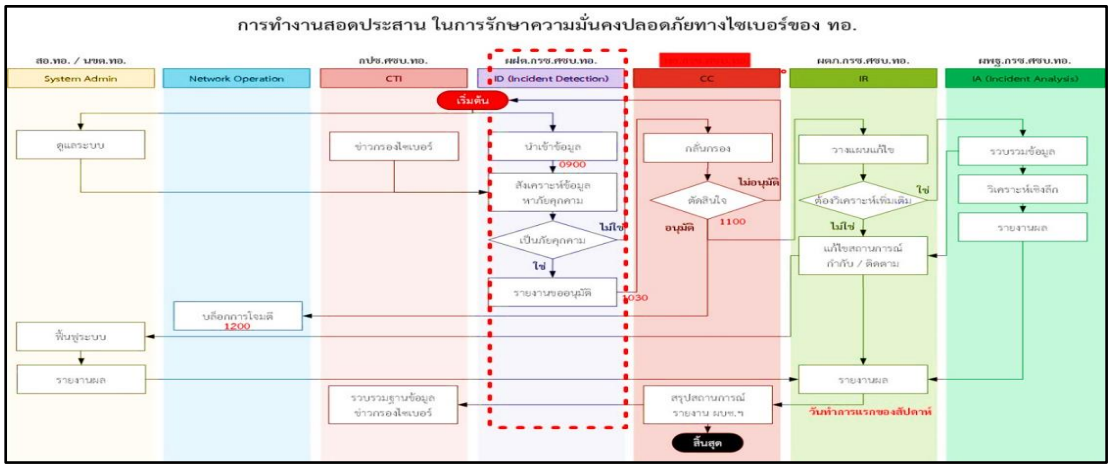
ภาพที่ ๑๔ ขั้นตอนการปฏิบัติในส่วนของผู้ดูแลระบบ ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ

๒.๑.๒ ข่าวกรองไซเบอร์ มีหน้าที่รวบรวมข่าวกรองไซเบอร์ และสรุปแจ้งเตือนให้กับ ชุดเฝ้าระวังทางไซเบอร์ เพื่อใช้ในการเฝ้าระวังและตรวจจับต่อไป



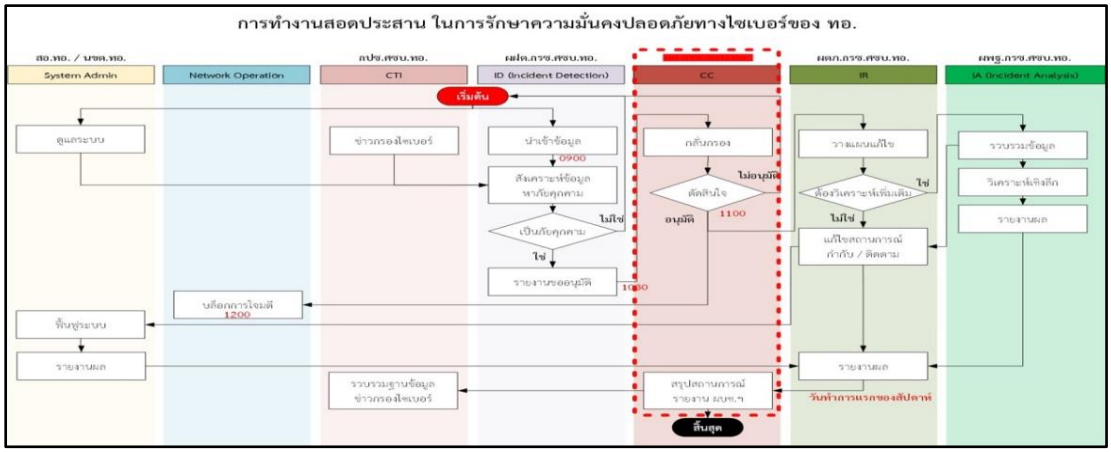
ภาพที่ ๑๕ ขั้นตอนการปฏิบัติในส่วนของข่าวกรองไซเบอร์ ฯ ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ

๒.๑.๓ ชุดเฝ้าระวังทางไซเบอร์ ศูนย์ยุทธการทางไซเบอร์ ศูนย์ปฏิบัติการกองทัพอากาศ มีหน้าที่ นำเข้าข้อมูล (Logs) จากเครื่องมือแจ้งเตือน สังเคราะห์ ตามสถานการณ์ภัยคุกคามทางไซเบอร์ รายงานให้ นายทหารฝ่ายเสนาธิการ ศูนย์ยุทธการทางไซเบอร์ ศูนย์ปฏิบัติการกองทัพอากาศ เพื่อพิจารณา และดำเนินการต่อไป



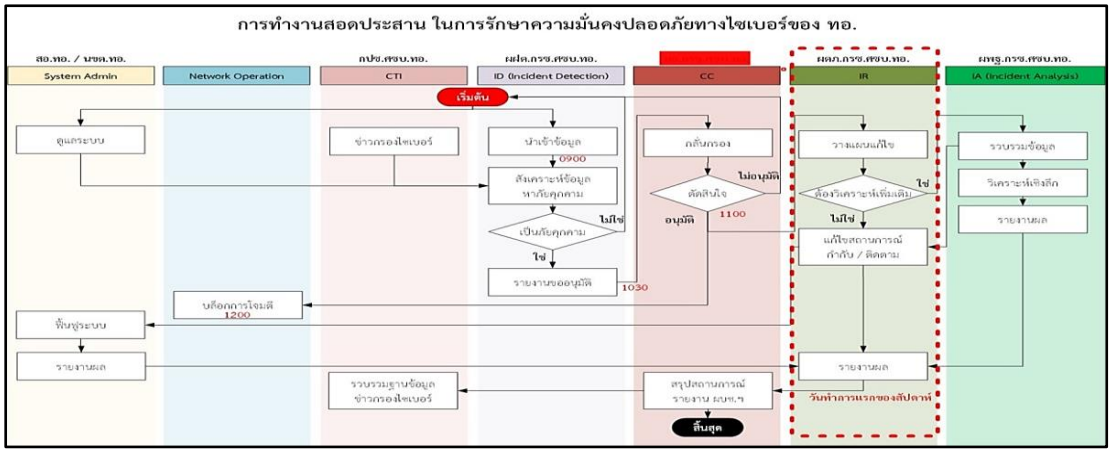
ภาพที่ ๑๖ ขั้นตอนการปฏิบัติในส่วนของชุดเฝ้าระวังทางไซเบอร์ ฯ ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ

๒.๑.๔ นายทหารฝ่ายเสนาธิการ ศูนย์ยุทธการทางไซเบอร์ ศูนย์ปฏิบัติการกองทัพอากาศ มีหน้าที่ประเมินสถานการณ์ทางไซเบอร์ ผลกระทบ และพิจารณาอนุมัติการดำเนินการตอบสนองภัยคุกคาม โดยจะดำเนินการสั่งการ ปิดกั้นไอพีแอดเดรส ที่เป็นภัยคุกคามให้ สอ.ทอ.ดำเนินการต่อไป



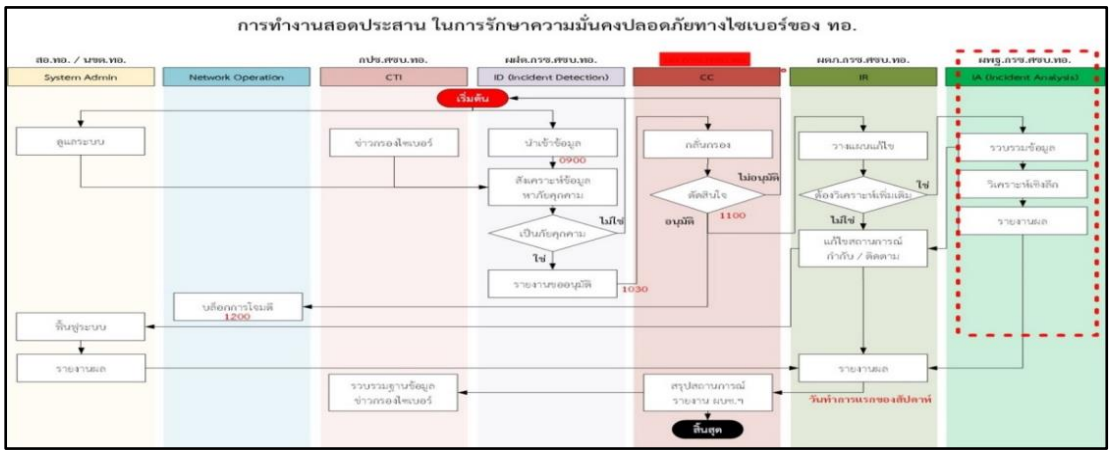
ภาพที่ ๑๗ ขั้นตอนการปฏิบัติในส่วนของนายทหารฝ่ายเสนาธิการ ฯ ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ

๒.๑.๕ ชุดเผชิญเหตุทางไซเบอร์ ศูนย์ยุทธการทางไซเบอร์ ศูนย์ปฏิบัติการกองทัพอากาศ มีหน้าที่วางแผนตอบสนองภัยคุกคามทางไซเบอร์ หากพบว่าระบบสารสนเทศใดได้รับผลกระทบ ให้นายทหารฟื้นฟูระบบ ติดต่อประสานผู้ดูแลระบบงานด้าน ฮาร์ดแวร์ ซอฟต์แวร์ หรือ ระบบสารสนเทศที่เกี่ยวข้องดำเนินการแก้ไข โดยให้คำแนะนำกระบวนการแก้ไขที่เหมาะสม และสรุปรายงานผู้บังคับบัญชา และหากต้องการวิเคราะห์เชิงลึก ให้นายทหารพิสูจน์หลักฐานทางดิจิทัลดำเนินการ

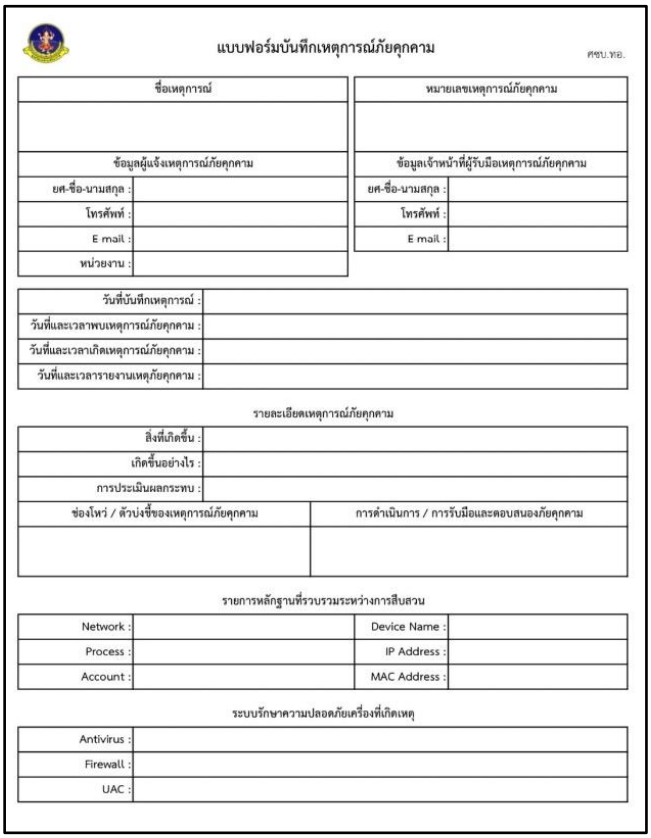


ภาพที่ ๑๘ ขั้นตอนการปฏิบัติในส่วนของชุดเผชิญเหตุทางไซเบอร์ ฯ ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ

๒.๑.๖ นายทหารพิสูจน์หลักฐานทางดิจิทัล ฯ มีหน้าที่ ดำเนินการรวบข้อมูล วิเคราะห์เชิงลึก และรายงานผลให้ผู้บังคับบัญชาทราบ เพื่อใช้เป็นข้อมูลให้ข่าวกรองไซเบอร์



ภาพที่ ๑๙ ขั้นตอนการปฏิบัติในส่วนของนายทหารพิสูจน์หลักฐานทางดิจิทัล ฯ ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ



แบบฟอร์มบันทึกเหตุการณ์ภัยคุกคาม

ศชบ.ทอ.

ชื่อเหตุการณ์	หมายเลขเหตุการณ์ภัยคุกคาม

ข้อมูลผู้แจ้งเหตุการณ์ภัยคุกคาม		ข้อมูลเจ้าหน้าที่ผู้รับมือเหตุการณ์ภัยคุกคาม	
ยศ-ชื่อ-นามสกุล :		ยศ-ชื่อ-นามสกุล :	
โทรศัพท์ :		โทรศัพท์ :	
E mail :		E mail :	
หน่วยงาน :			

วันที่บันทึกเหตุการณ์ :	
วันที่และเวลาพบเหตุการณ์ภัยคุกคาม :	
วันที่และเวลาเกิดเหตุการณ์ภัยคุกคาม :	
วันที่และเวลารายงานเหตุภัยคุกคาม :	

รายละเอียดเหตุการณ์ภัยคุกคาม

สิ่งที่เกิดขึ้น :	
เกิดขึ้นอย่างไร :	
การประเมินผลกระทบ :	

ช่องโหว่ / ตัวบ่งชี้ของเหตุการณ์ภัยคุกคาม	การดำเนินการ / การรับมือและตอบสนองภัยคุกคาม

รายการหลักฐานที่รวบรวมระหว่างการสืบสวน

Network :		Device Name :	
Process :		IP Address :	
Account :		MAC Address :	

ระบบรักษาความปลอดภัยเครื่องที่เกิดเหตุ

Antivirus :	
Firewall :	
UAC :	

ภาพที่ ๒๐ แบบฟอร์มบันทึกเหตุการณ์ภัยคุกคาม

๒.๒ ระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ความมุ่งหมายเพื่อให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ ทอ.เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ สามารถรับมือภัยคุกคามทางไซเบอร์ได้ โดยขอบเขตมีผลบังคับใช้กับผู้ปฏิบัติงานในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และผู้เกี่ยวข้อง ดังนี้ ผู้บังคับบัญชา ศยซบ.ศปก.ทอ., ชุดเฝ้าระวังทางไซเบอร์ ศยซบ.ศปก.ทอ., ชุดเผชิญเหตุทางไซเบอร์ ศยซบ.ศปก.ทอ. ชุดป้องปรามและโจมตีทางไซเบอร์ ศยซบ.ศปก.ทอ. และผู้ดูแลระบบ ทั้งด้านฮาร์ดแวร์ ซอฟต์แวร์ รวมทั้งระบบสารสนเทศ ที่เกี่ยวข้อง

๒.๒.๑ รายการปฏิบัติ

๒.๒.๑.๑ การปฏิบัติให้ยึดกระบวนการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๒.๑.๒ ชุดเฝ้าระวังทางไซเบอร์ ให้ดำเนินการนำเข้าข้อมูล และสังเคราะห์ภัยคุกคามทางไซเบอร์ ตามกระบวนการทำงาน ตามวงรอบ ดังนี้

๒.๒.๑.๒ (๑) สถานการณ์ภัยคุกคามทางไซเบอร์ระดับปกติ (สีขาว) ทุก ๆ ๒๔ ชม.

๒.๒.๑.๒ (๒) สถานการณ์ภัยคุกคามทางไซเบอร์ระดับไม่รุนแรง (สีเทา) ทุก ๆ ๒๔ ชม.

๒.๒.๑.๒ (๓) สถานการณ์ภัยคุกคามทางไซเบอร์ระดับรุนแรง (สีเหลือง) ทุก ๆ ๑๒ ชม.

๒.๒.๑.๒ (๔) สถานการณ์ภัยคุกคามทางไซเบอร์ระดับวิกฤต (สีแดง) ทุก ๆ ๘ ชม.

๒.๒.๒ ชุดเผชิญเหตุทางไซเบอร์ ให้สรุปสถานการณ์นำเรียน ผู้บังคับบัญชา ศยซบ.ศปก.ทอ. ตามกระบวนการทำงาน ตามวงรอบ ดังนี้

๒.๒.๒.๑ สถานการณ์ภัยคุกคามทางไซเบอร์ระดับปกติ (สีขาว) ทุก ๆ ๒๔ ชม.

๒.๒.๒.๒ สถานการณ์ภัยคุกคามทางไซเบอร์ระดับไม่รุนแรง (สีเทา) ทุก ๆ ๒๔ ชม.

๒.๒.๒.๓ สถานการณ์ภัยคุกคามทางไซเบอร์ระดับรุนแรง (สีเหลือง) ทุก ๆ ๑๒ ชม.

๒.๒.๒.๔ สถานการณ์ภัยคุกคามทางไซเบอร์ระดับวิกฤต (สีแดง) ทุก ๆ ๘ ชม.

๒.๒.๓ การปฏิบัติงาน ศปก.ทอ.ในมิติไซเบอร์

เมื่อมีภัยคุกคามทางไซเบอร์ต่อระบบเครือข่าย และสารสนเทศของ ศปก.ทอ.และ นขต.ทอ.ที่เกี่ยวข้อง จึงกำหนดแนวทางเพื่อให้ผู้เกี่ยวข้องใช้พิจารณากำหนดระดับสถานการณ์ภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น ๔ ระดับ และกำหนดสีระดับต่าง ๆ ดังนี้

๒.๒.๓.๑ ระดับปกติ (สีขาว) หมายถึง สถานการณ์ที่ภัยคุกคามส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญสารสนเทศของ ทอ. ในระดับที่ไม่ทำให้เกิดการทำงานที่ด้อยประสิทธิภาพหรือระบบสารสนเทศทั่วไปของ ทอ. ทั้งระบบหลักและระบบสำรองมิได้หยุดปฏิบัติงาน แต่ไม่สามารถทำงานได้ในบางระบบที่มิใช่ระบบสนับสนุนงานด้านยุทธการสถานการณ์ในระดับปกติ (สีขาว) โดยให้หน่วยเจ้าของ ระบบปฏิบัติตามกฎ ระเบียบ และคู่มือที่เกี่ยวข้อง หากมีสถานการณ์ภัยคุกคามทางไซเบอร์ให้แจ้งต่อ ฝทสส.ศปก.ทอ.และศูนย์ยุทธการทางไซเบอร์ ศปก.ทอ.โดยทันที

๒.๒.๓.๒ ระดับปกติ ระดับไม่รุนแรง (สีเทา) หมายถึง สถานการณ์ที่ภัยคุกคามส่งผลกระทบต่อระบบโครงสร้างพื้นฐานสำคัญสารสนเทศของ ทอ.ในระดับที่ทำให้เกิดการทำงานที่ด้อยประสิทธิภาพ หรือระบบสารสนเทศทั่วไปของ ทอ.อยู่ระดับที่ต้องหยุดปฏิบัติงานเพื่อแก้ไขปัญหา (โดยใช้เวลาไม่เกิน ๑ วัน) หรือเพิ่มมาตรการในการป้องกันทางไซเบอร์สถานการณ์ในระดับไม่รุนแรง (สีเทา) ให้ศูนย์ยุทธการทางไซเบอร์ ศปก.ทอ.ดำเนินการปฏิบัติต่อภัยคุกคามได้ทันทีพร้อมทั้งแจ้งให้ ฝทสส.ศปก.ทอ.พิจารณาดำเนินการ และรายงานผลการปฏิบัติให้ ผบ.ศปก.ทอ.ตามความเหมาะสมของสถานการณ์

๒.๒.๓.๓ ระดับรุนแรง (สีเหลือง) หมายถึง สถานการณ์ที่ภัยคุกคามส่งผลกระทบต่อระบบโครงสร้างพื้นฐานสำคัญสารสนเทศของ ทอ.ในระดับที่ต้องหยุดปฏิบัติงานเพื่อแก้ไขปัญหา (โดยใช้เวลาไม่เกิน ๑ วัน) หรือระบบสารสนเทศทั่วไปของ ทอ.อยู่ระดับที่สูญเสียการปฏิบัติงานและต้องจัดหาอุปกรณ์ทดแทน สถานการณ์ในระดับรุนแรง (สีเหลือง) ให้ศูนย์ยุทธการทางไซเบอร์ ศปก.ทอ.ดำเนินการปฏิบัติต่อภัยคุกคามได้ทันทีพร้อมทั้งแจ้งให้ ฝทสส.ศปก.ทอ.พิจารณาร่วมกับ ฝสธ.ศปก.ทอ. จัดประชุมคณะทำงานติดตามสถานการณ์ ศปก.ทอ.เพื่อดำเนินการตามแผนหรือคำสั่งยุทธการ ที่เกี่ยวข้อง

๒.๒.๓.๔ ระดับวิกฤต (สีแดง) หมายถึง สถานการณ์ที่ภัยคุกคามส่งผลกระทบต่อระบบโครงสร้างพื้นฐานสำคัญสารสนเทศ และระบบสารสนเทศทั่วไปของ ทอ.ในระดับที่สูญเสียการปฏิบัติงานเป็นวงกว้าง อุปกรณ์หลักของระบบโครงสร้างพื้นฐานสำคัญสารสนเทศเสียหายไม่สามารถซ่อมบำรุงได้ และต้องจัดหาอุปกรณ์ทดแทนทั้งหมด สถานการณ์ในระดับวิกฤต (สีแดง) ให้ศูนย์ยุทธการทางไซเบอร์ ศปก.ทอ.ดำเนินการปฏิบัติต่อภัยคุกคามได้ทันทีพร้อมทั้งแจ้งให้ ฝทสส.ศปก.ทอ.พิจารณาร่วมกับ ฝสธ.ศปก.ทอ. จัดประชุมคณะทำงานติดตามสถานการณ์ ศปก.ทอ.เพื่อดำเนินการตามแผนหรือคำสั่งยุทธการที่เกี่ยวข้อง

ทั้งนี้กำหนดให้ ฝทสส.ศปก.ทอ.พิจารณาร่วม ฝสธ.ศปก.ทอ.พิจารณาจัดการประชุมคณะทำงานติดตามสถานการณ์ ศปก.ทอ.เพื่อดำเนินการตามแผนหรือคำสั่งยุทธการที่เกี่ยวข้อง รวมทั้งพิจารณาเรียกผู้มีรายชื่อในบัญชีพร้อมเรียกด้านไซเบอร์ (Cyber On Call List) ร่วมปฏิบัติงาน ณ ศปก.ทอ.ตามความเหมาะสม

๒.๒.๔ ชุดปฏิบัติการป้องกันทางไซเบอร์ จำนวน ๒ ชุด มีรายละเอียด ดังนี้

๒.๒.๔.๑ ชุดเฝ้าระวังป้องกันทางไซเบอร์ (ศูนย์ยุทธการทางไซเบอร์ ศปก.ทอ.)

๒.๒.๔.๑ (๑) จัดนายทหารเฝ้าระวังป้องกันทางไซเบอร์ และเจ้าหน้าที่เฝ้าระวังป้องกันทางไซเบอร์ ตามความจำเป็นแต่ไม่เกินอัตราที่กำหนด

๒.๒.๔.๑ (๒) เฝ้าระวังระบบสารสนเทศของ ทอ.ทั้งระบบสารสนเทศด้านยุทธการ และระบบสารสนเทศด้านการสนับสนุน

๒.๒.๔.๑ (๓) ตรวจจับการบุกรุก/โจมตีระบบสารสนเทศ และรายงานให้ ฝทสส.ศปก.ทอ.ทราบทันที เมื่อตรวจพบพร้อมทั้งแจ้งเหตุการณ์ให้ผู้บังคับบัญชาทราบตามลำดับชั้น

๒.๒.๔.๑ (๔) รายงานผลการปฏิบัติให้ ฝทสส.ศปก.ทอ.ทราบ

๒.๒.๔.๒ ชุดเผชิญเหตุทางไซเบอร์ (ศูนย์ยุทธการทางไซเบอร์ ศปก.ทอ.)

๒.๒.๔.๒ (๑) จัดเตรียมอุปกรณ์สำหรับการปฏิบัติการตอบสนองกับเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ให้พร้อม ณ ที่ตั้งปกติ พร้อมเคลื่อนย้ายไปปฏิบัติการในพื้นที่ปฏิบัติการ เมื่อได้รับคำสั่ง

๒.๒.๔.๒ (๒) จัดนายทหารเผชิญเหตุทางไซเบอร์ และเจ้าหน้าที่เผชิญเหตุทางไซเบอร์ ตามความจำเป็นแต่ไม่เกินอัตราที่กำหนด และระงับการบุกรุก/โจมตีทางไซเบอร์โดยทันที

๒.๒.๔.๒ (๓) เก็บหลักฐานและตรวจพิสูจน์ทางดิจิทัล เพื่อให้ทราบถึงผู้บุกรุก/โจมตี ช่องทางที่ใช้ และวิธีการในการปฏิบัติ

๒.๒.๔.๒ (๔) ฟื้นฟูระบบที่ได้รับผลกระทบให้กลับคืนสู่สภาพปกติพร้อมใช้งานโดยเร็วที่สุด

๒.๒.๔.๒ (๕) รายงานผลการปฏิบัติให้ ฝทสส.ศปก.ทอ.ทราบ และเมื่อปฏิบัติการทั้งปวงแล้วเสร็จ ทั้งนี้ ให้หน่วยรับผิดชอบโครงสร้างพื้นฐานสำคัญสารสนเทศและระบบสารสนเทศของ ทอ.สามารถจัดกำลังพลสนับสนุนและช่วยเหลือชุดปฏิบัติการทางไซเบอร์ได้ตามความเหมาะสม เมื่อได้รับการร้องขอ

๒.๒.๕ การปฏิบัติหน้าที่เวรศูนย์ยุทธการทางไซเบอร์ ตรวจสอบความพร้อมใช้งานของระบบและอุปกรณ์ประจำศูนย์ยุทธการทางไซเบอร์ ฯ ตามคู่มือการปฏิบัติงานศูนย์ยุทธการทางไซเบอร์ ฯ

๒.๒.๖ เหตุการณ์สำคัญและการรายงาน

๒.๒.๖.๑ เหตุการณ์สำคัญ ได้แก่ การโจมตีทางไซเบอร์ที่กระทำต่อทรัพยากรทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒.๒.๖.๒ เมื่อเกิดเหตุการณ์สำคัญ ให้ น.เวร ศยซบ.ฯ รายงาน ผอ.ศยซบ.ฯ ทราบภายใน ๓๐ นาที พร้อมทั้งแจ้ง กรช.ศซบ.ทอ. ทราบด้วย โดยต้องบันทึกการรายงานเป็นหลักฐานทุกครั้ง

บทที่ ๓ เทคนิค และอุปกรณ์การป้องกันทางไซเบอร์

การโจมตีทางไซเบอร์มีหลากหลายรูปแบบ และมีการพัฒนาวิธีการหลบหลีกเครื่องมือป้องกันและอุปกรณ์ตรวจจับต่าง ๆ ดังนั้นเพื่อให้สามารถป้องกันการโจมตีทางไซเบอร์ มิให้ผู้ประสงค์ร้ายดำเนินการจนบรรลุวัตถุประสงค์ การป้องกันทางไซเบอร์จึงมีเทคนิค และอุปกรณ์ป้องกันภัยคุกคามทางไซเบอร์ เพื่อรับมือภัยคุกคามทางไซเบอร์รูปแบบต่าง ๆ ไม่ว่าจะเป็นวิธีการป้องกันแบบเจาะจง หรือเทคนิคการโจมตีหลากหลายรูปแบบ และลดผลกระทบจากความเสียหายที่จะเกิดขึ้น

๓.๑ เทคนิคการป้องกันทางไซเบอร์

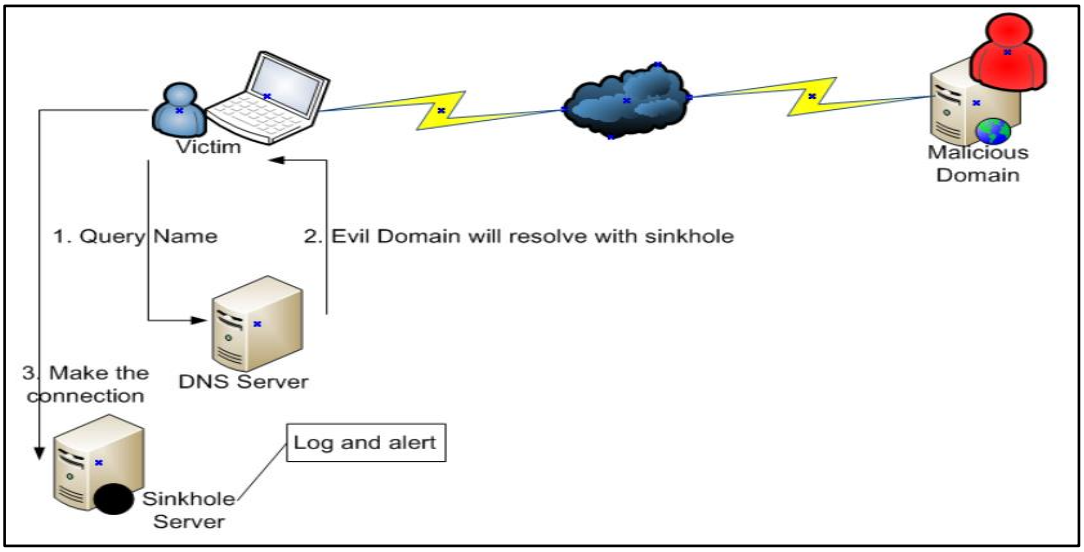
๓.๑.๑ DNS Sinkhole

DNS Sinkhole คือ การป้องกันการเชื่อมต่อระหว่างเครื่องที่ติดไวรัสและ C2 หรือ Malicious Domain โดยเมื่อมีการร้องขอ Resolve Name ที่มี Domain name อยู่ใน List Malicious Domain นั้น DNS Server จะตอบกลับ IP Address ที่เป็น Sinkhole Server ทำให้เครื่องที่ไวรัสติดต่อกับ C2 ไม่สำเร็จ โดยมีข้อจำกัด ดังนี้

๓.๑.๑.๑ ต้องมีการ Update Malicious Domain สม่ำเสมอ

๓.๑.๑.๒ หากถูก Malware แก้ไข Host File บนเครื่องที่ติดไวรัสจะไม่สามารถป้องกันได้

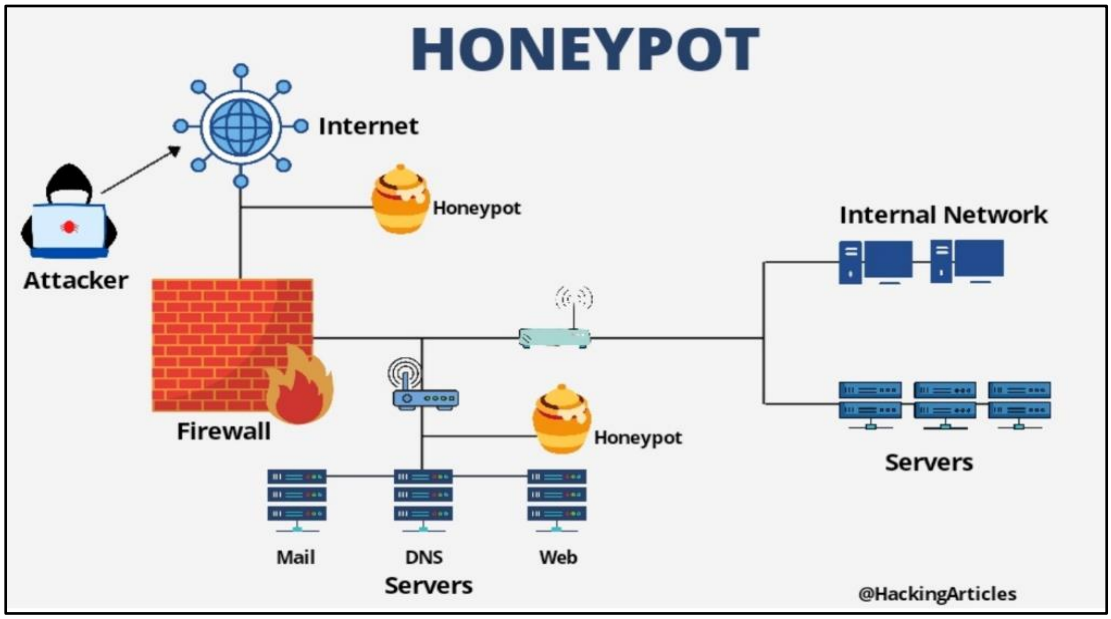
๓.๑.๑.๓ องค์กรต้องบังคับไม่ให้ DNS Traffic ของเครื่องลูกข่าย Resolve Name จากแหล่งอื่น



ภาพที่ ๒๑ DNS Sinkhole

๓.๑.๒ Honeypot

Honeypot เป็นเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายที่ตั้งขึ้น เพื่อดึงดูดและดักจับผู้ที่พยายามเข้าถึงเครือข่ายหรือระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต และยังสามารถใช้เพื่อตรวจจับและตรวจสอบกิจกรรมที่ไม่ได้รับอนุญาตเพื่อรวบรวมหลักฐานที่สามารถใช้ในการระบุตัวตนและดำเนินคดีกับอาชญากรไซเบอร์ โดยทั่วไปแล้ว Honeypot จะมีการกำหนดค่าให้เหมือนว่าเป็นระบบที่ใช้งานอยู่จริง แต่ถูกแยกออกจากระบบงานจริง เมื่อมีการโจมตีเข้ามายัง Honeypot ผู้โจมตีจะเชื่อว่ากำลังเข้าถึงระบบจริง และยังสามารถใช้ประโยชน์จาก Log ที่เกิดขึ้นจากการโจมตีนำมาวิเคราะห์เพื่อพัฒนาวิธีการป้องกันการโจมตี รวมถึงรูปแบบการโจมตีจากมัลแวร์ ตัวอย่างของการตั้ง Honeypot เช่น การตั้งค่าของบริการ FTP เพื่อให้สามารถเข้าถึงระบบโดยไม่ต้องผ่านการล็อกอินบนหน้าเว็บไซต์ เป็นต้น



ภาพที่ ๒๒ Honeypot

๓.๑.๓ Cryptography

Cryptography หรือ วิทยาการเข้ารหัสลับ เป็นการปกปิดข้อมูล โดยแปลงข้อความธรรมดา (Pain Text) ให้อยู่ในรูปแบบที่อ่านไม่ได้ (Cipher Text) โดยใช้กุญแจ (Key) ร่วมกับกระบวนการเข้ารหัส (Encryption) เมื่อผู้รับได้รับ Cipher Text ผู้รับจะใช้ Key และกระบวนการถอดรหัส (Decryption) เพื่อแปลง Cipher Text กลับไปเป็น Pain Text วัตถุประสงค์ของวิทยาการเข้ารหัสลับ มีดังนี้

๓.๑.๓.๑ Confidentiality (การรักษาความลับ) ใช้เพื่อรับประกันว่าผู้ที่ได้รับอนุญาตเท่านั้น ที่สามารถเข้าถึงข้อมูลได้

๓.๑.๓.๒ Integrity (การควบคุมข้อมูลให้ความถูกต้อง) ใช้ป้องกันการเปลี่ยนแปลงข้อมูลแบบไม่เหมาะสมและไม่ได้รับอนุญาต

๓.๑.๓.๓ Authentication (การพิสูจน์เอกลักษณ์บุคคล) ใช้พิสูจน์เอกลักษณ์บุคคลในการ สื่อสาร หรือใช้พิสูจน์ความถูกต้อง (ตรงกับต้นฉบับ) ของเอกสาร หรือของข้อมูลต่าง ๆ

๓.๑.๓.๔ Nonrepudiation (ไม่สามารถปฏิเสธความรับผิดชอบได้) เพื่อรับประกันว่าผู้ส่ง ข้อความ จะไม่สามารถปฏิเสธการส่งข้อความนั้นในภายหลังได้ และผู้รับก็ไม่สามารถ ปฏิเสธการได้ข้อความนั้นได้เช่นกัน

๓.๑.๔ DHCP Snooping

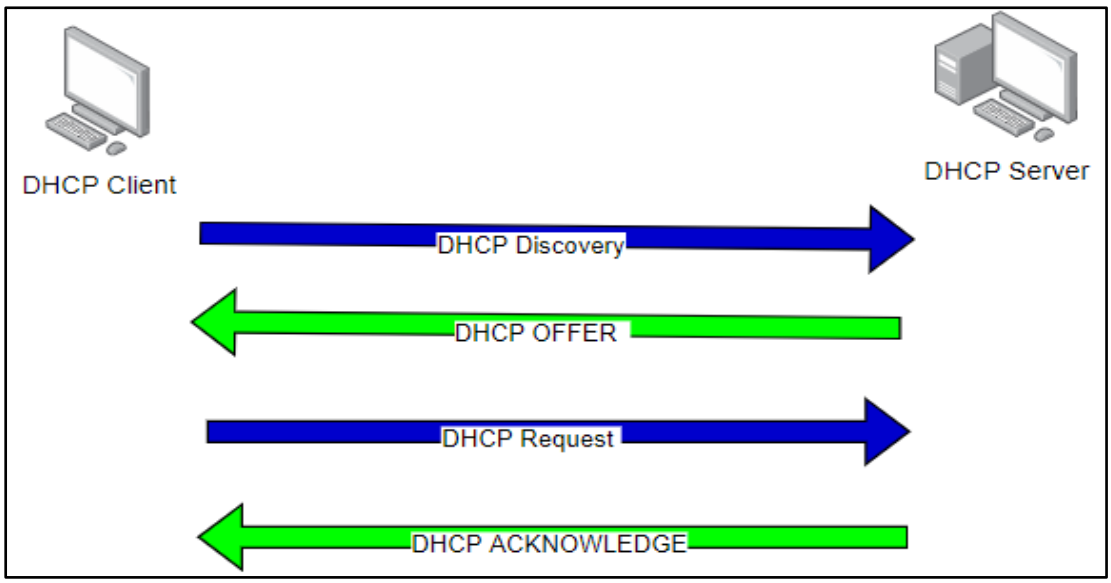
๓.๑.๔.๑ Dynamic Host Configuration Protocol (DHCP) คือรูปแบบแจกจ่ายค่าที่ใช้ในการเชื่อมต่อระบบเครือข่าย เช่น IP Address, Subnet Mask, Gateway และ DNS เป็นต้น โดยมีหลักการทำงาน ดังนี้

๓.๑.๔.๒ DHCP Client ต้องการข้อมูลการเชื่อมต่อของระบบเครือข่ายจะทำการส่ง DHCP Discovery แบบ Broadcast ออกมา

๓.๑.๔.๓ DHCP Server ได้รับ DHCP discovery จะทำการจอง IP Address และส่งข้อมูลต่าง ๆ ด้วย DHCP OFFER ไปยังเครื่องลูกข่ายที่ทำการร้องขอมา

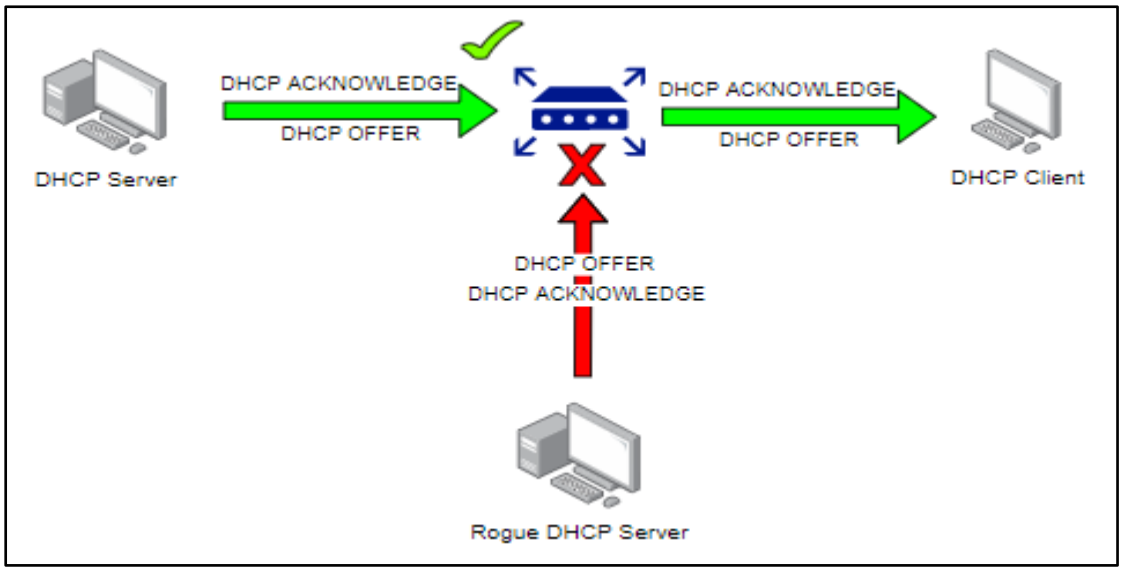
๓.๑.๔.๔ DHCP Client ได้รับ DHCP OFFER จะทำการตั้งค่าข้อมูลเครือข่ายตามที่ได้รับมาและส่ง DHCP Request กลับไปที่ DHCP Server

๓.๑.๔.๕ DHCP Server ได้รับ DHCP REQUEST จะทราบว่า DHCP Client นำเอา IP Address และไปใช้เรียบร้อย และจะทำการส่ง DHCP ACKNOWLEDGE กลับไป



ภาพที่ ๒๓ DHCP Snooping

ดังนั้นหากมีการติดตั้ง DHCP Server และเชื่อมต่อในระบบเครือข่ายมากกว่า ๑ เครื่อง จะทำให้ Client บางเครื่องได้รับ IP Address รวมถึงข้อมูลของระบบเครือข่ายที่ไม่ถูกต้อง ทำให้สามารถเปลี่ยนเส้นทางการสื่อสารข้อมูลได้ ถูกเป็นการโจมตีประเภทหนึ่ง ทำให้มีการพัฒนาการป้องกันการตั้ง DHCP Server ซ้อนในระบบเครือข่าย โดยใช้ชื่อว่า DHCP Snooping DHCP Snooping เป็นเทคนิคการป้องกันการแอบตั้ง DHCP Server ขึ้นมาในระบบเครือข่าย โดยมักจะเปิดใช้การป้องกันที่อุปกรณ์เครือข่าย มีหลักการทำงาน คือ กำหนดค่า Port ที่ DHCP Server จริงใช้อยู่ ซึ่งอุปกรณ์เครือข่ายจะทำการ Drop DHCP OFFER และ DHCP ACKNOWLEDGE ที่ได้รับจาก Port อื่น ๆ ทำให้ Client ไม่ได้ค่า IP Address หรือข้อมูลอื่น ๆ จาก DHCP Server ที่ไม่ได้รับอนุญาต



ภาพที่ ๒๔ DHCP Server

๓.๑.๕ Multi-Factor Authentication (MFA) เป็นกระบวนการรักษาความปลอดภัยในการเข้าใช้งานระบบ หรือเข้าถึงข้อมูล โดยผู้ใช้งานต้องมีการยืนยันตัวตนด้วยปัจจัยตั้งแต่ ๒ อย่างขึ้นไป ที่แตกต่างกัน เช่น รหัสผ่าน และ PIN ที่ได้รับจาก SMS MFA เป็นต้น มีปัจจัยที่ใช้ในการยืนยันตัวตน ๓ กลุ่มใหญ่ คือ

๓.๑.๕.๑ Knowledge Factor การยืนยันตัวตนด้วยสิ่งที่เรารู้ เช่น รหัสผ่าน หรือ PIN เป็นต้น

๓.๑.๕.๒ Possession Factor การยืนยันตัวตนด้วยสิ่งที่เรามี เช่น SMS มือถือ การยืนยันผ่าน Application บนมือถือ หรือ USB Token เป็นต้น

๓.๑.๕.๓ Inherence Factor หรือ Biometric คือการใช้ส่วนต่าง ๆ ของร่างกาย ที่ระบุตัวตน เช่น ลายนิ้วมือ เรตินา สแกนใบหน้า หรือการจดจำเสียง เป็นต้น

ภาพที่ ๒๕ Multi-Factor Authentication

๓.๑.๖ เทคนิคการตรวจจับภัยคุกคามบนระบบเครือข่าย

การตรวจตรวจจับภัยคุกคามบนระบบเครือข่ายจะนิยมใช้ อุปกรณ์ประเภท Intrusion Detection System (IDS) โดยมีหน้าที่ในการตรวจสอบและรายงานข้อมูลที่ตรวจพบการตรวจจับ แบ่งเป็น ๒ ประเภทหลัก คือ

๓.๑.๖.๑ Signature-Based คือ การตรวจจับผู้บุกรุกเครือข่ายโดยเปรียบเทียบ Packet ที่ถูกส่งผ่านเครือข่าย โดยระบบจะมีข้อมูลรูปแบบการโจมตี หรือตัวบ่งชี้การโจมตี หากตรวจพบ Packet ที่มีรูปแบบตรงตามรูปแบบการโจมตี ระบบจะทำการแจ้งเตือน ดังนั้นการตรวจจับประเภทนี้จะมีประสิทธิภาพในการตรวจจับการโจมตีหรือช่องโหว่ที่ทราบรูปแบบหรือข้อมูลการโจมตีแล้ว ซึ่งจะไม่สามารถตรวจจับการโจมตีรูปแบบใหม่ๆ ที่ไม่รู้จักมาก่อนได้

๓.๑.๖.๒ Behavior-Based คือ การตรวจจับการบุกรุกเครือข่ายที่อาจเกิดขึ้นโดยการวิเคราะห์พฤติกรรมของการรับส่งข้อมูลเครือข่ายและผู้ใช้ และเปรียบเทียบกับชุดของพฤติกรรมที่เป็นการใช้งานตามปกติ โดยระบบจะตรวจสอบการรับส่งข้อมูลเครือข่ายและพฤติกรรมของผู้ใช้ เมื่อเวลาผ่านไป ระบบจะจดจำพฤติกรรมที่เป็นการใช้งานปกติและใช้เป็นจุดอ้างอิง หากมีการใช้งานเบี่ยงเบนจากปกติจะทำการแจ้งเตือนและมีการเรียนรู้พฤติกรรมทั่วไปบนเครือข่าย เช่น รูปแบบการรับส่งข้อมูลปกติ รูปแบบการเข้าถึงระบบของผู้ใช้ และการใช้ทรัพยากร เป็นต้น ซึ่งจะใช้เป็นมาตรฐานในการระบุความผิดปกติ ทั้งนี้จะมีประสิทธิภาพในการตรวจจับรูปแบบการโจมตีที่ไม่รู้จักหรือรูปแบบใหม่ หรือ Zero-day และ APT แต่อาจมีอัตราการตรวจพบที่ผิดพลาดและแจ้งเตือนที่เป็นกิจกรรมที่ผิดปกติแต่ไม่ใช่การบุกรุกหรือโจมตี (False Positive) ค่อนข้างสูง

๓.๒ อุปกรณ์การป้องกันทางไซเบอร์

๓.๒.๑ Security Information and Event Management (SIEM)

คือ ระบบที่มีการรวมความสามารถระหว่าง Security Event Management (SIM) ที่เป็นระบบการจัดการข้อมูลความปลอดภัย และ Security Information Management (SEM) ระบบการจัดการเหตุการณ์ความปลอดภัย โดยใช้ความสัมพันธ์ทางสถิติเพื่อช่วยในการตรวจจับภัยคุกคาม ซึ่ง SIEM เป็นระบบที่รวบรวมข้อมูลด้าน Security จากอุปกรณ์ Hardware Software และระบบต่าง ๆ ในเครือข่าย เช่น Client, Server, Domain controllers, Firewall, IDS, Event และอื่น ๆ เป็นต้น นำมาจัดเก็บ เปลี่ยนรูปแบบ ตรวจสอบ วิเคราะห์ แสดงผล และแจ้งเตือน เพื่อให้องค์กรสามารถนำข้อมูลด้านความมั่นคงปลอดภัยจาก Hardware หรือ Software ที่มีอยู่มาวิเคราะห์ร่วมกัน ทำให้สามารถ ช่วยค้นหาปัญหา ภัยคุกคาม หรือการโจมตีที่เกิดขึ้น และเป็นแหล่งที่สามารถใช้ตรวจสอบเหตุการณ์การโจมตีที่เกิดขึ้นในเชิงลึก เพื่อระบุถึงสาเหตุ ความเสียหาย และความเสี่ยง ทำให้สามารถตอบสนอง ต่อภัยคุกคามความปลอดภัยที่อาจเกิดขึ้นได้อย่างรวดเร็ว

SIEM ได้รับการออกแบบมาเพื่อระบุภัยคุกคามด้านความปลอดภัยที่อาจเกิดขึ้น เช่น การติดมัลแวร์ การบุกรุกเครือข่าย และการละเมิดข้อมูล เป็นต้น และแจ้งเตือนไปยังเจ้าหน้าที่รักษาความปลอดภัย เพื่อดำเนินการต่อเหตุการณ์ต่อไป นอกจากนี้ยังสามารถใช้เพื่อติดตามกิจกรรมของผู้ใช้ ตรวจสอบการปฏิบัติตามนโยบายความปลอดภัย และให้การวิเคราะห์ทางนิติวิทยาศาสตร์เพื่อช่วยให้เข้าใจสาเหตุของเหตุการณ์ด้านความปลอดภัย โดยองค์กรที่ต้องการใบรับรองมาตรฐานด้านความปลอดภัย เช่น ISO 27000, ISO 27001, ISO 27002 และ ISO 27003 เป็นต้น ซึ่งต้องมีการจัดการและการเก็บรักษาบันทึก การจัดการเคส และการตรวจสอบการบังคับใช้ตามนโยบาย ทั้งนี้จึงเลือกใช้ระบบ SIEM เพื่อให้สามารถปฏิบัติตามมาตรฐานด้านความปลอดภัยได้อย่างครบถ้วน

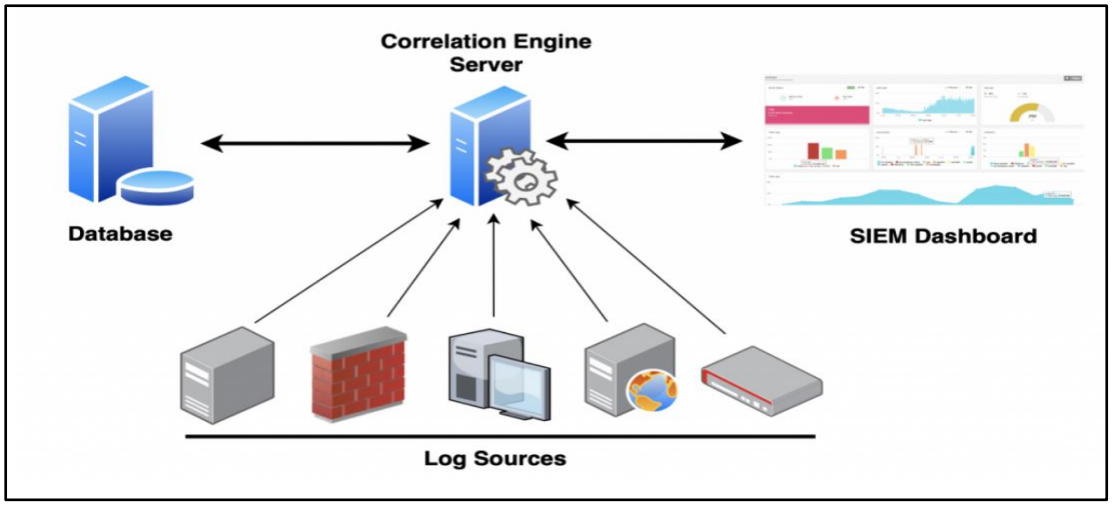
หลักการทำงานของ SIEM จะมีการรับ Log จากแหล่งต่าง ๆ และเพื่อนำมาวิเคราะห์ข้อมูล โดยมีการกระบวนการ ดังนี้

๓.๒.๑.๑ การรวบรวมข้อมูล (Data Collection) เป็นการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ของระบบหรืออุปกรณ์เครือข่ายทั้งหมด เช่น ข้อมูล Log ของระบบปฏิบัติการ, Antivirus, IDS, IPS, Server และ Firewall เป็นต้น เพื่อบันทึกข้อมูลเก็บไว้ ก่อนนำไปวิเคราะห์หาภัยคุกคามที่อาจจะเกิดขึ้น

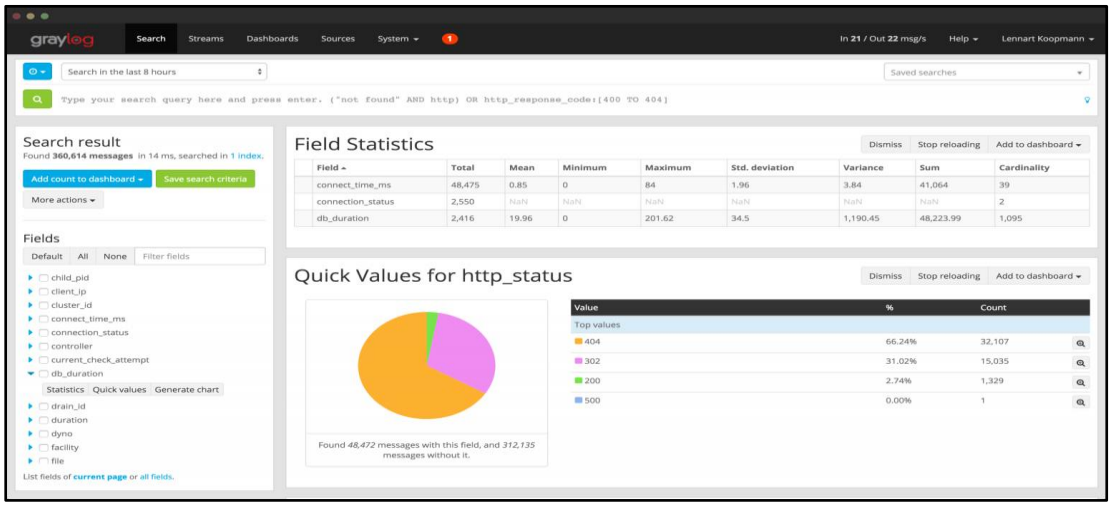
๓.๒.๑.๒ การกำหนดนโยบาย (Policies) เพื่อให้ SIEM รู้ถึงพฤติกรรมการดำเนินการในสถานการณ์ปกติ และเหตุการณ์ด้านความปลอดภัยที่อาจเกิดขึ้น โดย SIEM สามารถสร้างเงื่อนไขการแจ้งเตือน รายงาน และแดชบอร์ด เพื่อให้สอดคล้องกับสิ่งที่หน่วยงานต้องการ

๓.๒.๑.๓ การจัดการความสัมพันธ์ (Data consolidation and correlation) SIEM จัดข้อมูล แปลงข้อมูล วิเคราะห์ข้อมูล และหาความสัมพันธ์ของเหตุการณ์จาก Log ต่าง ๆ ที่ได้รับมาเพื่อระบุสิ่งที่อาจจะเป็นคุกคามทางไซเบอร์

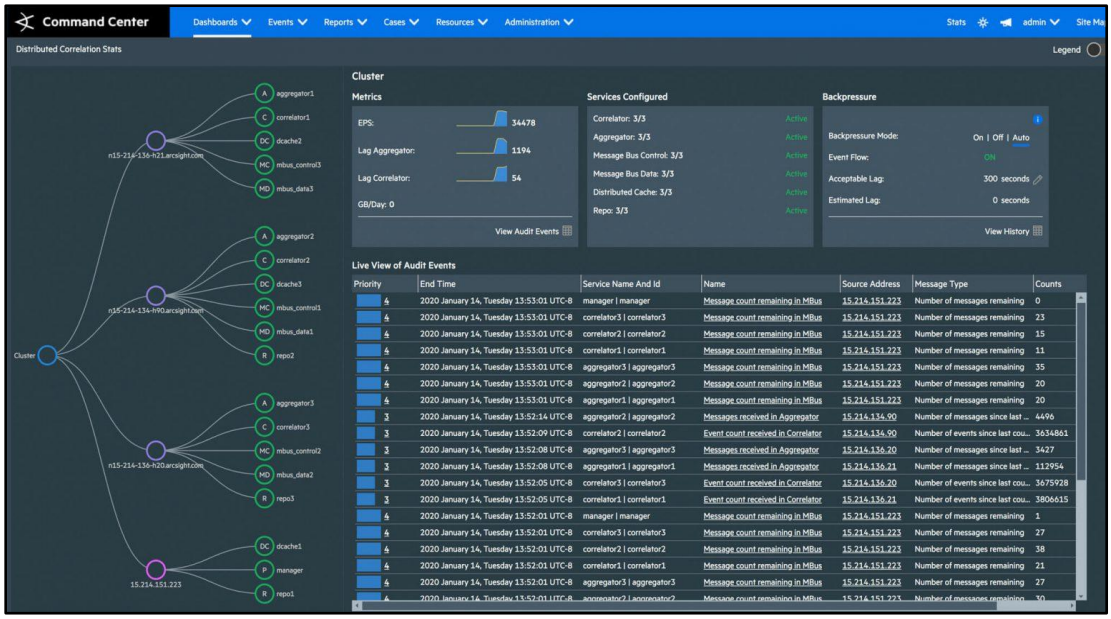
๓.๒.๑.๔ การแจ้งเตือน (Alerts) หากมีเหตุการณ์หรือข้อมูลที่คาดว่าจะเกิดเหตุการณ์ภัยคุกคามไซเบอร์ระบบจะแจ้งเตือนไปยัง ส่วนงานที่ระบุไว้เพื่อให้ทราบและตรวจสอบต่อไป



ภาพที่ ๒๖ ตัวอย่าง SIEM Platforms

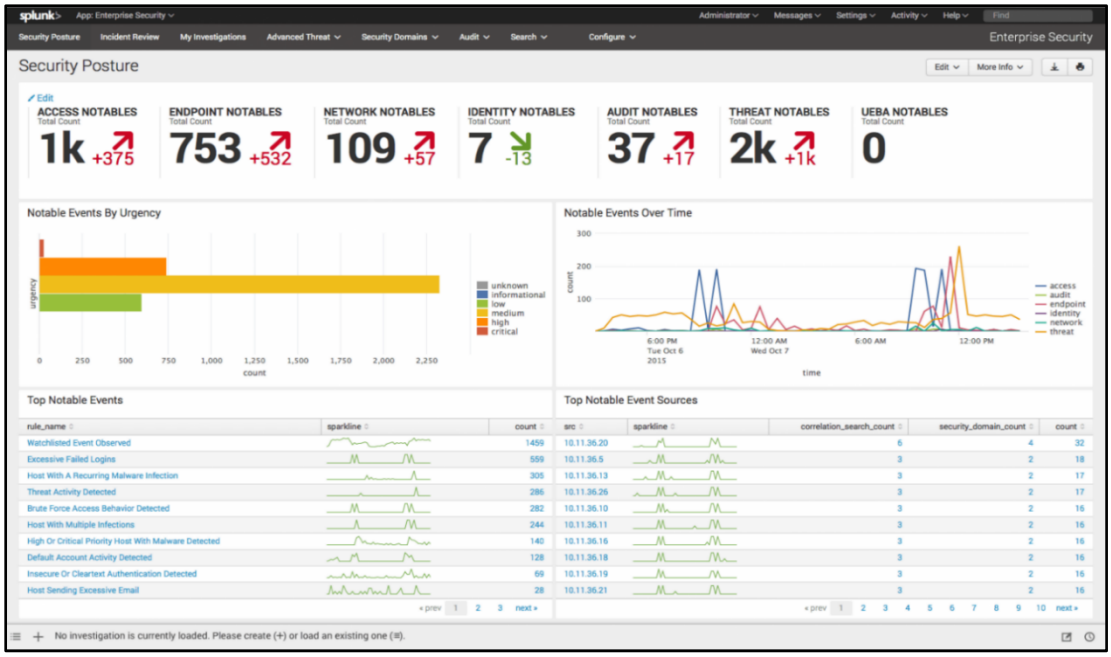


ภาพที่ ๒๗ Gray Log



ภาพที่ ๒๘ ArcSight

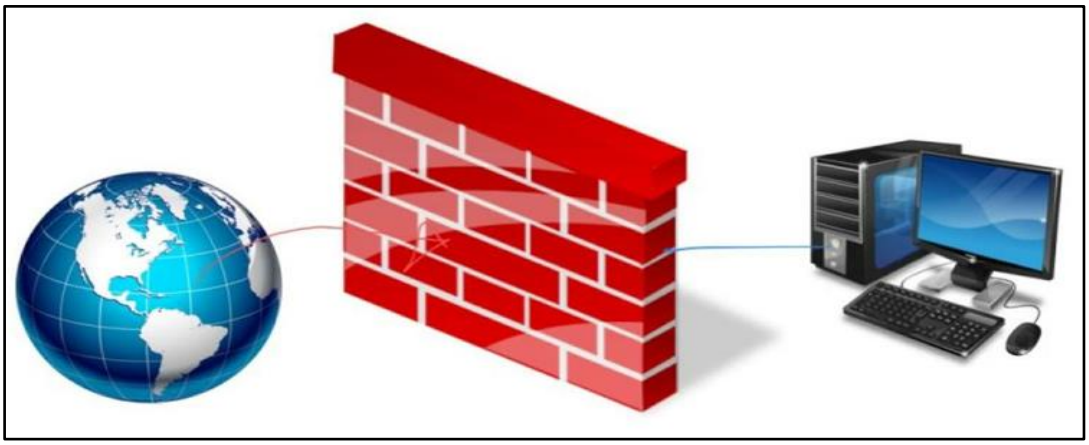
ภาพที่ ๒๙ Qradar



ภาพที่ ๓๐ Splunk

๓.๒.๒ Firewall

Firewall เป็นซอฟต์แวร์ หรือฮาร์ดแวร์ที่สำหรับป้องกันเครือข่ายจากการบุกรุกของแฮ็กเกอร์ หรือชุดคำสั่งที่อาจก่อให้เกิดความเสียหายต่อระบบและเครือข่ายได้ เปรียบเสมือนกำแพงป้องกันไฟที่จะลุกลามเข้ามายังเมืองได้ Firewall ที่ดีจะต้องสามารถระบุพฤติกรรมของการใช้งานเครือข่าย ที่อาจจะก่อให้เกิดความเสียหายแก่ระบบและเครือข่ายได้ รวมไปถึงความสามารถในการทำงานร่วมกันกับอุปกรณ์ และระบบตรวจจับการบุกรุกอื่น ๆ ในเครือข่ายได้อย่างมีประสิทธิภาพ มีการรายงานผลและตอบสนองที่รวดเร็ว อีกทั้งยังต้องมีระบบภายใน Firewall ต้องเป็นมิตรต่อผู้ดูแลระบบ (User friendly)



ภาพที่ ๓๑ Firewall

๓.๒.๒.๑ ความสำคัญของ ไฟร์วอลล์ (Firewall)

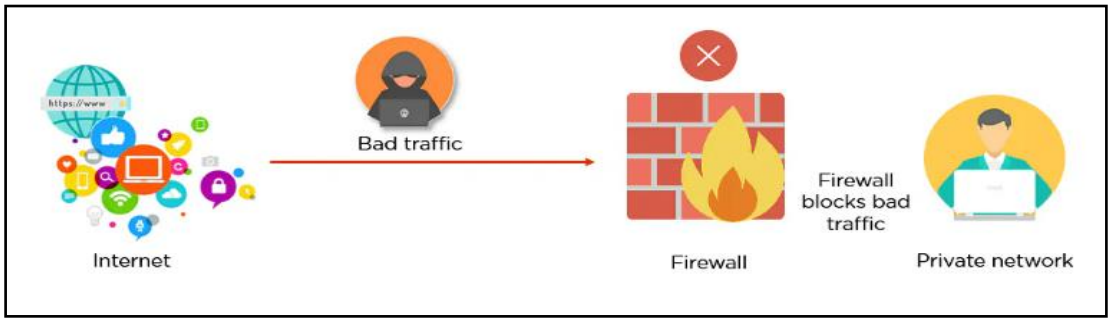
๓.๒.๒.๑ (๑) ช่วยลดช่องโหว่การรักษาความปลอดภัยเครือข่ายขององค์กร วัตถุประสงค์หลักของไฟร์วอลล์ คือเพื่อป้องกันการโจมตีการรักษาความปลอดภัยเครือข่ายหรือการโจมตีของแฮ็กเกอร์ ไฟร์วอลล์ฮาร์ดแวร์สามารถกำหนดค่าหรือกฎเฉพาะที่สามารถจดจำและปิดกั้นไวรัสและมัลแวร์ และยังสามารถป้องการเข้าถึงจากภายนอกที่ไม่ได้รับอนุญาตอีกด้วย

๓.๒.๒.๑ (๒) ช่วยตรวจสอบและควบคุมการใช้อินเทอร์เน็ต นอกเหนือจากการตรวจสอบการรับส่งข้อมูลขาเข้าแล้ว ไฟร์วอลล์ฮาร์ดแวร์ยังสามารถใช้เพื่อตรวจสอบและปิดกั้นการรับส่งข้อมูลขาออกจากภายในองค์กร โดยการนำกฎที่กำหนดมาใช้ ทางเทคโนโลยีสารสนเทศสามารถปิดกั้นการเข้าถึงโซเชียลมีเดีย ระบุตัวตน และหยุดการเข้าถึงเว็บไซต์ที่ไม่เหมาะสมได้ รวมถึงยังสามารถจำกัดการใช้งานอินเทอร์เน็ตทั้งในและนอกเวลาทำการอีกด้วย โดยกระบวนการนี้จะช่วยเพิ่มผลลัพธ์ที่ดีในการทำงานและในที่สุดแล้วก็จะช่วยเพิ่มผลกำไรทางธุรกิจได้อีกด้วย

๓.๒.๒.๑ (๓) ใช้ในการตรวจสอบเครือข่ายเพื่อป้องกันการโจมตีหรือการละเมิด ปัจจุบัน ยังไม่มีไฟร์วอลล์ที่สามารถป้องกันการคุกคามทางไซเบอร์ได้ทั้งหมด ทุกเครือข่ายก็อาจถูกโจมตีหรือละเมิดได้ ไฟร์วอลล์ฮาร์ดแวร์มีความสามารถในการตรวจสอบการรับส่งข้อมูลเครือข่ายขาเข้าและขาออกทั้งหมด รวมถึงแจ้งเตือนองค์กร ผู้จัดการด้านเทคโนโลยีสารสนเทศ เมื่อมีกิจกรรมที่ไม่ได้รับอนุญาตเกิดขึ้น สิ่งนี้จะช่วยให้เกิดการตอบสนองได้อย่างรวดเร็วเมื่อมีการละเมิดหรือโจมตีเกิดขึ้น ซึ่งจะสามารถกำหนดค่าและจัดการการแจ้งเตือนภายในแผงควบคุมไฟร์วอลล์ซอฟต์แวร์ โดยส่วนใหญ่แล้วไฟร์วอลล์ฮาร์ดแวร์มักกำหนดค่าให้มีการแจ้งเตือนผ่านทางอีเมลหรือข้อความ

๓.๒.๒.๑ (๔) ช่วยปกป้องอีเมลและชื่อเสียงขององค์กรโดยสามารถกำหนดค่าไฟร์วอลล์ฮาร์ดแวร์เพื่อป้องกันอีเมลเซิร์ฟเวอร์ ถ้าหากแฮ็กเกอร์เข้าถึงเครือข่ายได้อาจขโมยข้อมูลจากอีเมลเซิร์ฟเวอร์ และใช้ส่งสแปมไปยังบัญชีอีเมลของผู้ติดต่อ การกระทำนี้อาจส่งผลให้เกิดความเสียหายต่อชื่อเสียงขององค์กรได้

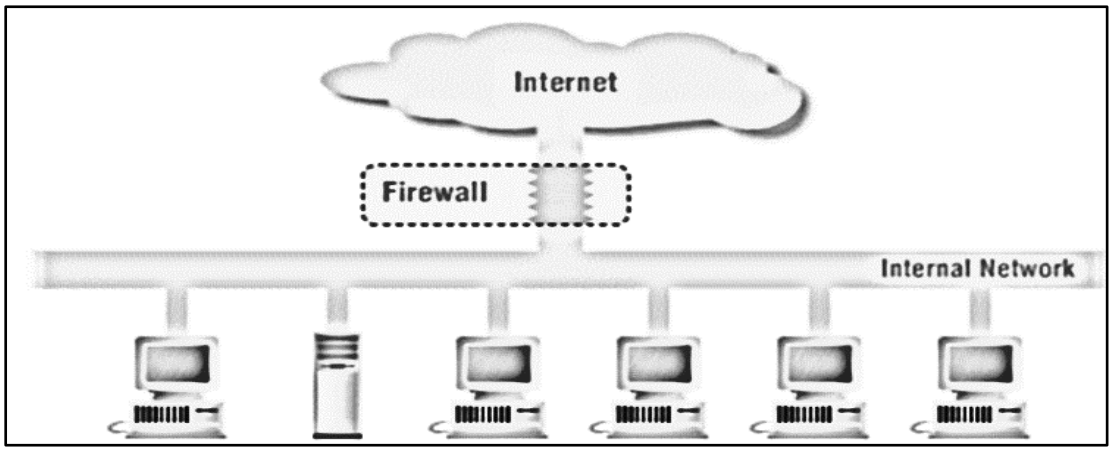
๓.๒.๒.๑ (๕) การเคลื่อนที่สามารถเชื่อมต่อกับเครือข่ายขององค์กร และเข้าถึงทรัพยากรผ่านการเชื่อมต่อที่เข้ารหัสเฉพาะ ซึ่งจะทำให้เครือข่ายมีความปลอดภัยเพิ่มขึ้นอีกขั้นโดยสามารถตั้งค่าหรือกำหนดไฟร์วอลล์ให้เหมาะสม และช่วยไม่ให้เกิดการดักจับข้อมูลขององค์กรและข้อมูลส่วนตัวจากบุคคลภายนอกได้



ภาพที่ ๓๒ การสร้างเครือข่ายส่วนตัวเสมือน

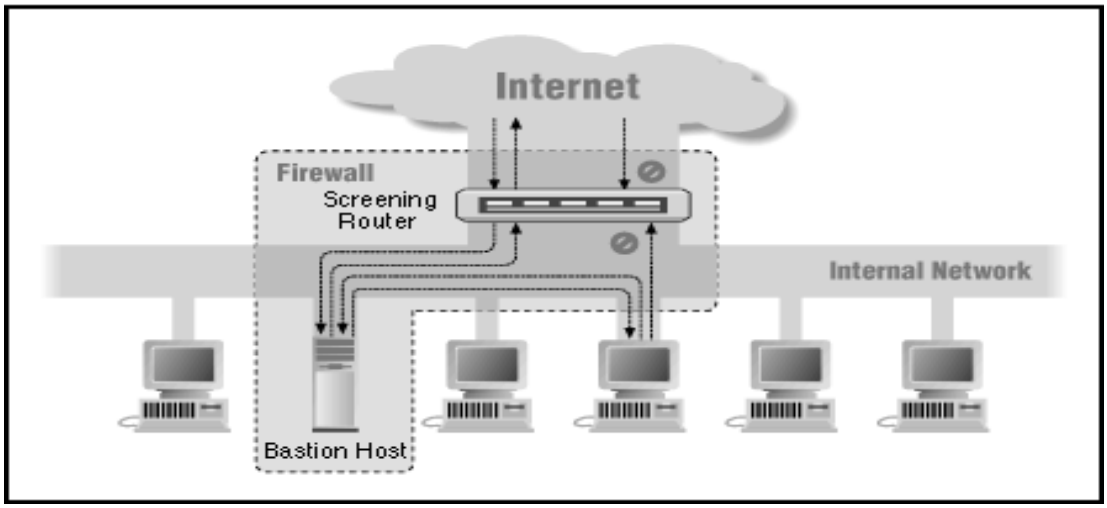
๓.๒.๒.๒ สถาปัตยกรรมของระบบความปลอดภัยเครือข่าย Firewall แบ่งออกเป็น ๓ รูปแบบ ดังนี้

๓.๒.๒.๒ (๑) Single Box Architecture เป็นโครงสร้างแบบง่าย ๆ ที่มีองค์ประกอบทำหน้าที่เป็นไฟร์วอลล์เพียงอันเดียวตั้งอยู่ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก ข้อดีของวิธีนี้ก็คือการที่มีเพียงจุดเดียวที่หน้าที่ไฟร์วอลล์ทั้งหมด ควบคุมการเข้าออกของข้อมูล ทำให้ดูแลได้ง่าย เป็นจุดสนใจในการดูแลความปลอดภัยเครือข่าย ในทางกลับกันข้อเสียของวิธีนี้ก็คือ การที่มีเพียงจุดเดียวนี้ ทำให้มีความเสี่ยงสูง หากมีการตั้งค่าผิดพลาดหรือมีช่องโหว่เพียงเล็กน้อย การผิดพลาดเพียงจุดเดียวอาจทำให้ระบบถูกเจาะได้



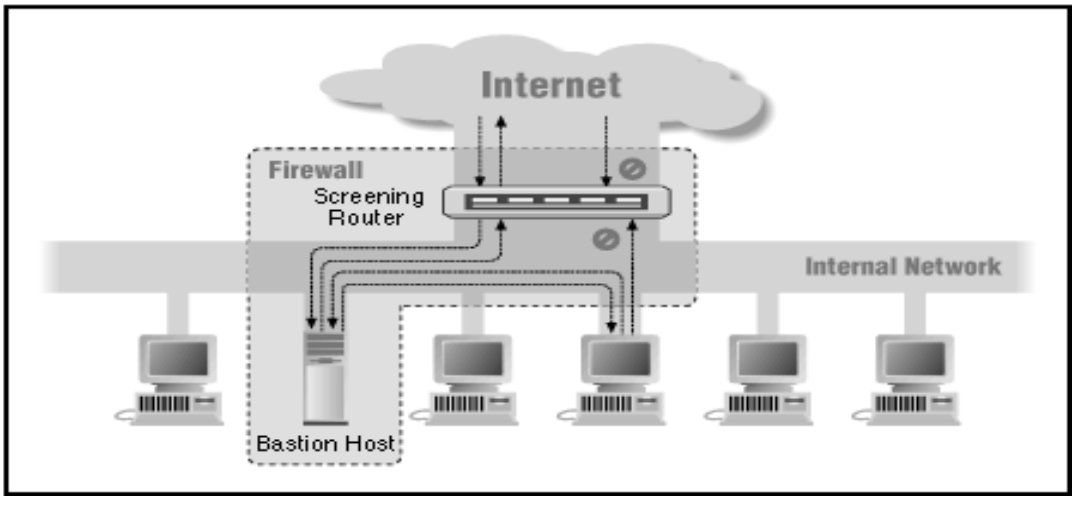
ภาพที่ ๓๓ สถาปัตยกรรมของระบบความปลอดภัยเครือข่าย Firewall

๓.๒.๒.๒ (๒) Screened Host Architecture จะมีโฮสต์ซึ่งให้บริการ Proxy เหมือนกับใน Single Box Architecture ที่เป็น Dual-homed Host แต่จะต่างกันตรงที่ว่า โฮสต์นั้นจะอยู่ที่เครือข่ายภายใน ไม่ต่ออยู่กับเครือข่ายภายนอกอื่น ๆ (ดังนั้นก็ไม่จำเป็นที่จะต้องใช้ Dual Homed Host) และจะมี เราเตอร์ที่ทำหน้าที่ Packet Filtering ช่วยบังคับให้เครื่องภายในเครือข่ายต้องติดต่อเซอร์วิสผ่าน Proxy โดยไม่ยอมให้ติดต่อใช้เซอร์วิสจากภายนอกโดยตรง และก็ให้ภายนอกเข้าถึงได้เฉพาะ Bastion Host (โฮสต์ที่มีความเสี่ยงสูงต่อการถูกโจมตี มักจะเป็นโฮสต์ที่เปิดให้บริการกับอินเตอร์เน็ต ดังนั้นโฮสต์นี้ต้องมีการดูแลเป็นพิเศษ) เท่านั้น



ภาพที่ ๓๔ Screened Host Architecture

๓.๒.๒.๒ (๓) Multi-Layer Architecture เป็นสถาปัตยกรรมแบบหลายชั้น ไฟร์วอลล์จะเกิดขึ้นจากองค์ประกอบหลาย ๆ ส่วน ทำหน้าที่ประกอบกันขึ้นเป็นระบบ วิธีการนี้สามารถเพิ่มความปลอดภัยได้มาก เนื่องจากเป็นการลดความเสี่ยงต่อความผิดพลาดที่อาจเกิดขึ้น ถ้าหากมีไฟร์วอลล์เพียงจุดเดียวแล้วมีเกิดความผิดพลาดเกิดขึ้น ระบบทั้งหมดก็จะเป็นอันตราย แต่ถ้ามีการป้องกันหลายชั้น หากในชั้นแรกถูกเจาะ ก็อาจจะมีความเสียหายเพียงบางส่วน ส่วนที่เหลือระบบก็ยังคงมีชั้นอื่น ๆ ในการป้องกันอันตราย และยังลดความเสี่ยงได้โดยการที่แต่ละชั้นนั้นมีการใช้เทคโนโลยีที่แตกต่างกัน เพื่อให้เกิดความหลากหลาย เป็นการหลีกเลี่ยงการโจมตีหรือช่องโหว่ที่อาจมีในเทคโนโลยีชนิดใดชนิดหนึ่ง โดยทั่วไปแล้วสถาปัตยกรรมแบบหลายชั้นจะเป็นการต่อกันเป็นซีรีย์โดยมี Perimeter Network (หรือบางทีเรียกว่า DMZ Network) อยู่ตรงกลาง เรียกว่า Screened Subnet Architecture เป็นสถาปัตยกรรมที่มีการเพิ่ม Perimeter Network เข้าไปกั้นระหว่างอินเทอร์เน็ตกับเครือข่ายภายในไม่ให้เชื่อมต่อกันโดยตรง ทำให้เน็ตเวิร์กภายในมีความปลอดภัยมากขึ้น



ภาพที่ ๓๕ Multi-Layer Architecture

๓.๒.๒.๓ ประเภทของระบบความปลอดภัยเครือข่าย Firewall สามารถแบ่งประเภทได้ ๒ ชนิด ได้แก่ แบ่งตามระดับชั้น และแบ่งตามการใช้งาน โดยทั่วไปนั้นนิยมแบ่งตามการใช้งานซึ่งแบ่งได้ ๔ ประเภทดังนี้

๓.๒.๒.๓ (๑) Packet Filtering Firewall เป็น Firewall ที่ทำหน้าที่ในการกลั่นกรองแพ็กเก็ตโดยจะทำการตรวจสอบจากเฮดเดอร์ในชั้น Network Layer หมายเลขพอร์ตและไอพีแอดเดรสจากต้นทาง และปลายทาง รวมถึงชนิดของโพรโตคอลที่ใช้ ถ้าไม่มีอะไรผิดปกติก็จะส่งแพ็กเก็ตนั้นต่อไปหากตรวจสอบแล้วไม่ถูกต้องก็จะบล็อกทันที

๓.๒.๒.๓ (๒) Circuit-Level Gateway Firewall เป็น Firewall ที่ทำหน้าที่เพิ่มเติมจาก Packet Filtering Firewall ไม่ได้เพียงแค่ตรวจสอบเพียงอย่างเดียวแต่จะมีการพิจารณาเปรียบเทียบจากแพ็กเก็ตที่ได้บันทึกเอาไว้ก่อนหน้านี้ เพื่อที่จะดูว่าแพ็กเก็จใดเข้ามาก่อนหลัง

๓.๒.๒.๓ (๓) Application-Level Firewall เป็นซอฟต์แวร์ที่ติดตั้งบน Firewall ระหว่าง ๒ เครือข่ายโดย Proxy จะทำหน้าที่เพิ่มความมั่นคงปลอดภัยให้กับเครือข่ายเพราะมีการตรวจสอบการทำงานในระดับชั้นแอพพลิเคชันเลเยอร์

๓.๒.๒.๓ (๔) Firewall โดย Firewall ประเภทนี้จะเป็นการเพิ่มเทคโนโลยี Stateful Inspection เข้าไปกับ Packet Filtering โดยจะไม่ได้พิจารณาแค่การตรวจสอบแพ็กเก็ตแต่จะดูแพ็กเก็ตที่เข้ามาก่อนหน้าว่าเป็นแพ็กเก็ตที่เข้ามาใหม่หรือกำลังเชื่อมต่ออยู่

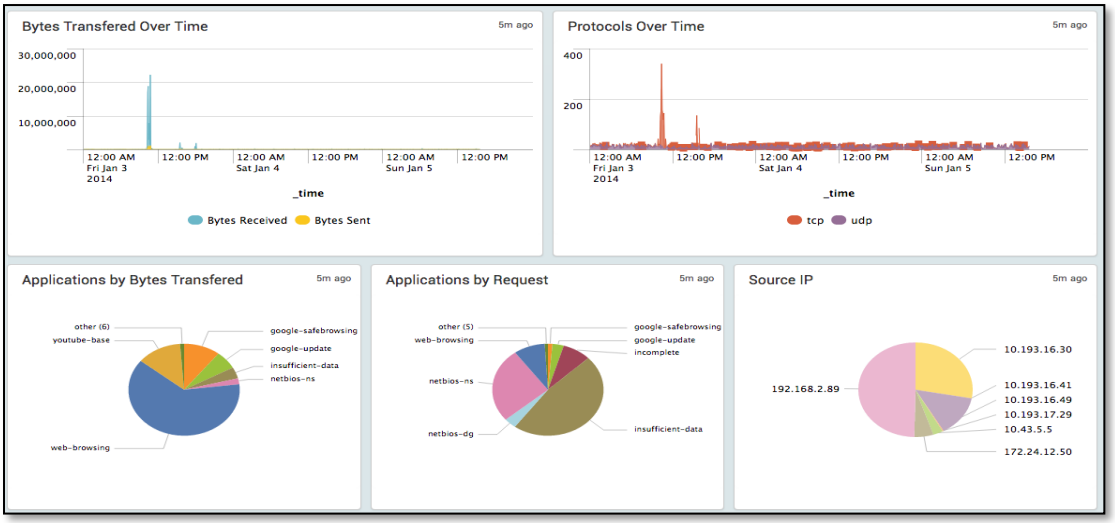
๓.๒.๒.๔ คุณลักษณะของระบบความปลอดภัยเครือข่าย

๓.๒.๒.๔ (๑) บังคับใช้นโยบายด้านความปลอดภัย โดยการกำหนดกฎให้กับ Firewall ว่าจะอนุญาตหรือไม่ให้ใช้บริการรูปแบบใด

๓.๒.๒.๔ (๒) ทำให้การพิจารณาดูแลและการตัดสินใจด้านความปลอดภัยของระบบเป็นไปได้ง่ายขึ้น เนื่องจากการติดต่อทุกชนิดกับ Network ภายนอกจะต้องผ่าน Firewall การดูแลที่จุดนี้เป็นการดูแลความปลอดภัยในระดับของ Network (Network-based Security)

๓.๒.๒.๔ (๓) บันทึกข้อมูล กิจกรรมต่างๆ ที่ผ่านเข้าออก Network ได้อย่างมีประสิทธิภาพ ป้องกันเครือข่ายบางส่วนจากการเข้าถึงของเครือข่ายภายนอก เช่นถ้าหากเรามีบางส่วนที่ต้องการให้ภายนอกเข้ามาใช้เซอร์วิส (เช่นถ้ามีเว็บเซิร์ฟเวอร์) แต่ส่วนที่เหลือไม่ต้องการให้ภายนอกเข้ามากรณีเช่นนี้เราสามารถใช้ Firewall ช่วยได้

๓.๒.๒.๔ (๔) Firewall บางชนิด สามารถป้องกันไวรัสได้ โดยจะทำการตรวจไฟล์ที่โอนย้ายผ่านทางโปรโตคอล HTTP, FTP และ SMTP



ภาพที่ ๓๖ ตัวอย่างของ Firewall ได้แก่ Palo alto, Pfsense และ Fortigate

๓.๒.๒.๕ ข้อจำกัดของ Firewall

๓.๒.๒.๕ (๑) ภัยคุกคามที่เกิดจากเครือข่ายภายใน ไม่สามารถป้องกันได้ เนื่องจากอยู่ภายในเครือข่ายเอง ไม่ได้ผ่าน Firewall เข้ามา

๓.๒.๒.๕ (๒) ภัยคุกคามจากภายนอกที่ไม่ได้ผ่าน Firewall เช่น การ Dial-up เข้ามายังเครือข่ายภายในโดยตรง เป็นต้น

๓.๒.๒.๕ (๓) ภัยคุกคามรูปแบบใหม่ที่เกิดขึ้น เนื่องจากมีการค้นพบช่องโหว่ที่ยังไม่ถูกเปิดเผย ซึ่งจะไม่สามารถไว้ใจ Firewall ด้วยการติดตั้งและตั้งค่าเพียงครั้งเดียว จะต้องมีการอัปเดตและตรวจสอบการตั้งค่าอย่างสม่ำเสมอ

๓.๒.๒.๕ (๔) ไวรัส ถึงแม้จะมี Firewall บางชนิดที่สามารถป้องกันไวรัสได้ แต่ก็ยังไม่มี Firewall ชนิดใดที่สามารถตรวจสอบไวรัสได้ในทุก ๆ โปรโตคอล

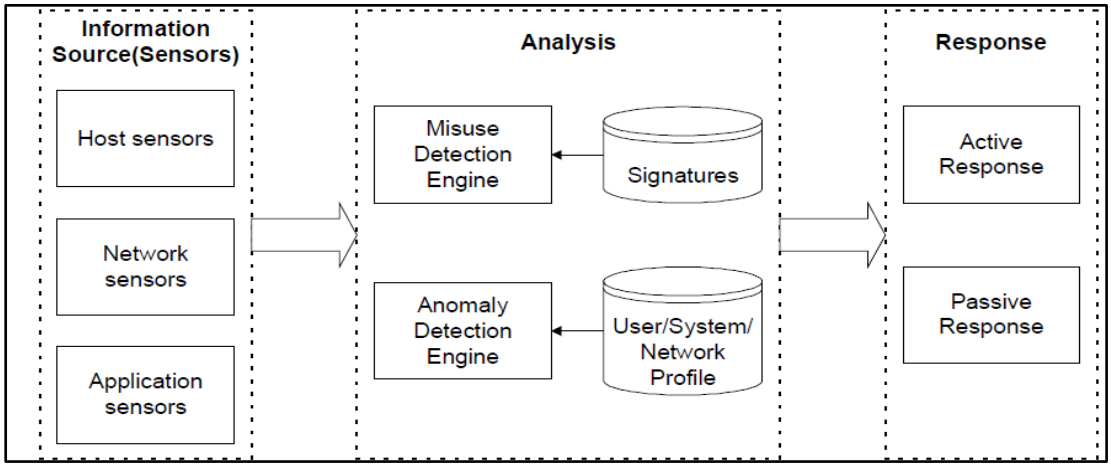
๓.๒.๓ Intrusion Detection System (IDS) ระบบตรวจจับการบุกรุกเป็นฮาร์ดแวร์หรือซอฟต์แวร์ที่ช่วยในการตรวจสอบ และติดตามการจราจรของแพ็กเก็ตในเครือข่าย รวมถึงการวิเคราะห์พฤติกรรมของผู้ใช้เพื่อตรวจสอบความผิดปกติและนำไปพยากรณ์เพื่อตัดสินใจว่ามีการบุกรุกและดำเนินการแจ้งเตือนไปยังระบบหรือผู้ดูแลระบบ

๓.๒.๓.๑ ความสำคัญของระบบตรวจจับการบุกรุก เมื่อคำนึงถึงเรื่องความปลอดภัยของคอมพิวเตอร์มักเป็นการยากในการมองภาพที่ชัดเจนว่า อะไรที่จะบ่งบอกได้ว่าการใช้งานคอมพิวเตอร์มีความปลอดภัย จากปัญหาภัยคุกคามและการโจมตีในรูปแบบต่าง ๆ ที่ส่งผลกระทบต่อความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย ดังนั้นจึงจำเป็นจะต้องมีกระบวนการในการตรวจจับการโจมตีหรือการบุกรุก เพื่อที่จะได้รับทราบและทำการแก้ไขปัญหาดังกล่าวได้ทันท่วงที โดยระบบตรวจจับการบุกรุก (IDS) จะแบ่งประเภทจากแหล่งที่มาของข้อมูลที่ใช้ในการวิเคราะห์เพื่อตรวจจับการบุกรุกแต่ละรูปแบบ จุดเด่นและจุดด้อยของ IDS ในแต่ละประเภท ซึ่งแนวทางและวิธีการต่าง ๆ ที่ใช้ในการตรวจจับการบุกรุกและคุณลักษณะของระบบตรวจจับการบุกรุกที่ดีนั้นจะมีองค์ประกอบพื้นฐาน ๓ ส่วน ดังนี้

๓.๒.๓.๑ (๑) Information Source (Sensor) ข้อมูลเหตุการณ์และข้อมูลการทำงานจากแหล่งข้อมูลต่าง ๆ นำไปใช้ในการวิเคราะห์เพื่อตัดสินใจว่า เมื่อใดที่มีการบุกรุกเกิดขึ้น โดยแหล่งข้อมูลเหล่านี้จะนำมาจากข้อมูลในระดับต่าง ๆ ของระบบ เช่น ข้อมูลในระดับเครือข่าย ระดับเครื่องคอมพิวเตอร์ และโปรแกรมประยุกต์ที่มีการใช้งานอยู่ในระบบ เป็นต้น

๓.๒.๓.๑ (๒) Analysis เป็นส่วนที่ทำหน้าที่ในการจัดการและวิเคราะห์ข้อมูลที่ได้รับจากแหล่งข้อมูลต่าง ๆ แล้วตัดสินว่าเหตุการณ์หรือการกระทำใดที่บ่งชี้ว่ากำลังมีการบุกรุกเกิดขึ้นหรือได้มีการบุกรุกเกิดขึ้นแล้วในระบบ โดยแนวทางที่ใช้ในการวิเคราะห์มีสองรูปแบบ คือ Anomaly Detection และ Misuse Detection

๓.๒.๓.๑ (๓) Response เป็นชุดของการกระทำเมื่อระบบตรวจจับการบุกรุกตรวจจับได้ว่ามีการบุกรุกเกิดขึ้น โดยการกระทำเหล่านี้สามารถจัดกลุ่มได้เป็นการกระทำแบบ Active และ Passive โดยที่การกระทำแบบ Active จะก่อให้มีการกระทำอื่น ๆ ที่จะตอบสนองต่อเหตุการณ์การบุกรุกนั้นโดยอัตโนมัติ เช่น การปรับค่าของเราเตอร์หรือไฟร์วอลล์ให้ปิดกั้นการเชื่อมต่อที่ส่งมาจากผู้บุกรุก และปิดกั้นพอร์ตหรือโปรโตคอลที่ถูกใช้ผู้บุกรุก เป็นต้น ส่วนการกระทำแบบ Passive จะเป็นการรายงานหรือแจ้งเตือนการบุกรุกไปยังบุคคลที่รับผิดชอบเพื่อแก้ไขปัญหา โดยอาศัยข้อมูลที่ได้รับรายงาน

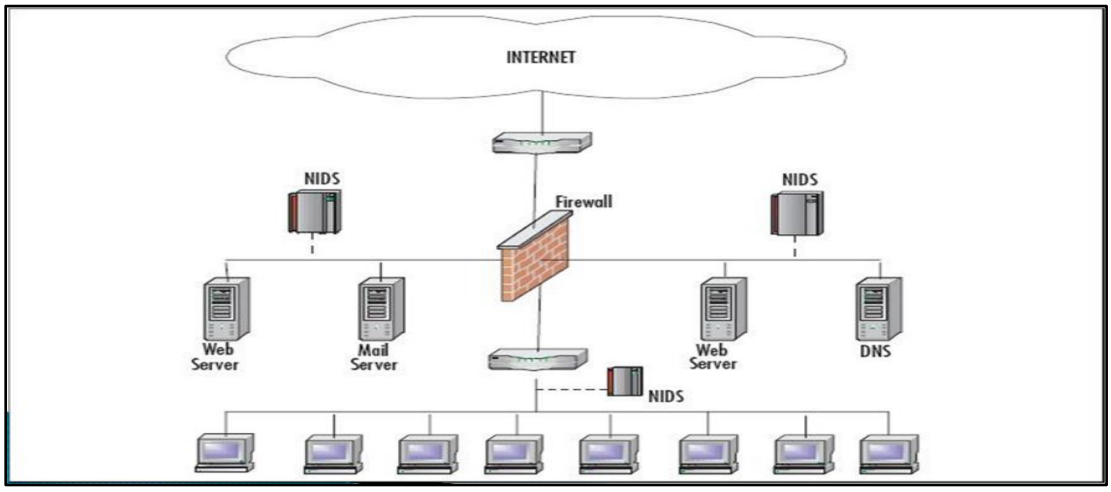


ภาพที่ ๓๗ ความสำคัญของระบบตรวจจับการบุกรุก

๓.๒.๓.๒ ประเภทของระบบตรวจจับการบุกรุก การจัดประเภทของระบบตรวจจับการบุกรุกสามารถแบ่งได้หลายรูปแบบ โดยใช้หลักเกณฑ์ต่าง ๆ เช่น แหล่งข้อมูลที่นำมาวิเคราะห์แนวทางในการตรวจจับการบุกรุก และช่วงระยะเวลาที่ทำการวิเคราะห์การบุกรุกหลังจากเกิดเหตุการณ์ขึ้น เป็นต้น

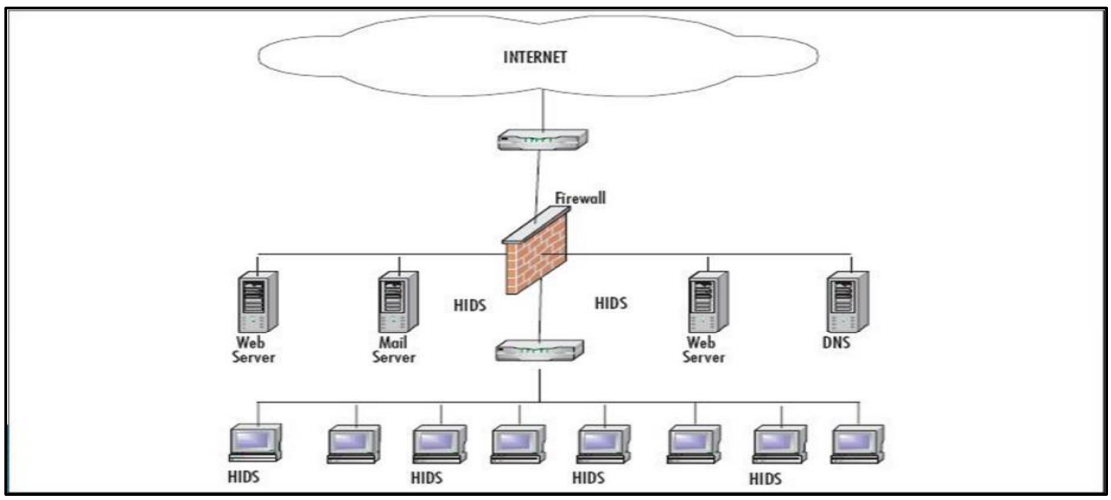
๓.๒.๓.๒ (๑) Network Base Intrusion Detecting System (NIDS) เป็นระบบตรวจจับการบุกรุกที่ติดตามและวิเคราะห์ Packet ที่รับส่งกันในเครือข่ายเพื่อดูว่ามี ผู้บุกรุกหรือความผิดปกติเกิดขึ้นหรือไม่ โดยจะดักจับข้อมูลบน Network Segment หรืออุปกรณ์สวิตช์ ดังนั้น NIDS หนึ่งระบบก็จะสามารถติดตามข้อมูลบนเครือข่ายซึ่งจะมีผลกับหลาย ๆ เครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่ในเครือข่ายเดียวกันและตรวจจับการบุกรุกที่จะเกิดขึ้นกับเครื่องเหล่านั้นได้ด้วย ทั้งนี้

Packet จะถูกตรวจจับโดยตัวดักจับ (Sensor) และวิเคราะห์ว่าเข้ากับรูปแบบหรือร่องรอยการบุกรุก (Signature) ที่กำหนดไว้ในฐานข้อมูลการบุกรุกของ NIDS หรือไม่ เช่น ระบบเฝ้าตรวจสอบการร้องขอการเชื่อมต่อบน TCP ที่พยามยามจะเชื่อมต่อมายังพอร์ตต่าง ๆ ของเครื่องเป้าหมาย เป็นต้น โดย NIDS นั้นอาจจะถูกติดตั้งบนเครื่องเป้าหมายเองและคอยตรวจทุกแพ็กเก็ตของตัวเองหรืออาจจะถูกติดตั้งบนเครื่องที่แยกอยู่ต่างหากเพื่อคอยตรวจจับทุกแพ็กเก็ตในเครือข่ายที่เครื่องเป้าหมายอยู่ก็ได้



ภาพที่ ๓๘ สถาปัตยกรรมของ Network-based IDS (NIDS)

๓.๒.๓.๒ (๒) Host-Base Intrusion Detecting System (HIDS) เป็นระบบตรวจจับการบุกรุกที่รวบรวมข้อมูลจากแต่ละเครื่องคอมพิวเตอร์ เพื่อตรวจสอบว่าโปรแกรมหรือผู้ใช้คนใดที่ทำให้เกิดการบุกรุกขึ้นในระบบ และผลของการบุกรุกเป็นอย่างไร ระบบ HIDS ส่วนใหญ่จะเก็บรวบรวมข้อมูลจากบันทึกการทำงานของระบบปฏิบัติการแล้วนำข้อมูลเหล่านั้นมาวิเคราะห์ด้วยวิธีการและเทคนิคต่าง ๆ เพื่อค้นหาเหตุการณ์ผิดปกติหรือการบุกรุกที่เกิดขึ้น



ภาพที่ ๓๙ สถาปัตยกรรมของ Host-based IDS (HIDS)

๓.๒.๓.๒ (๓) Application-Base Intrusion Detecting System ระบบ ตรวจจับ การบุกรุกประเภทนี้จะมีการทำงานคล้ายกับ HIDS แต่จะรวบรวมข้อมูลจากการทำงานของโปรแกรมประยุกต์ที่ทำงานบนเครื่องคอมพิวเตอร์ มาใช้ในการวิเคราะห์เพื่อตรวจสอบว่ามีพฤติกรรมผิดปกติหรือการใช้สิทธิ์เกินขอบเขตที่กำหนดไว้ของผู้ใช้หรือไม่รวบรวมข้อมูลจากบันทึกการทำงานของระบบปฏิบัติการแล้วนำข้อมูลเหล่านั้นมาวิเคราะห์ด้วยวิธีการและเทคนิคต่าง ๆ เพื่อค้นหาเหตุการณ์ผิดปกติหรือการบุกรุกที่เกิดขึ้น

๓.๒.๓.๓ หลักการทำงานของระบบตรวจหาการบุกรุก

๓.๒.๓.๓ (๑) การตรวจหาการใช้งานที่ผิด (Misuse Detection) หรือ (Signature-Based) เป็นการตรวจหารูปแบบการบุกรุกด้วยการวิเคราะห์พฤติกรรมหรือเหตุการณ์ที่เกิดขึ้นในระบบเครือข่าย โดยการเปรียบเทียบพฤติกรรมหรือเหตุการณ์ที่เข้ามาในเครือข่าย ณ เวลาขณะนั้นกับพฤติกรรม หรือเหตุการณ์ที่เป็นการบุกรุกซึ่งจัดเก็บไว้ในฐานข้อมูลระบบ หากเปรียบเทียบแล้วตรงกันแสดงว่าพฤติกรรมหรือเหตุการณ์นั้นเป็นการบุกรุกระบบก็จะแจ้งเตือนให้ผู้รับผิดชอบระบบทราบมี ๒ ชนิด คือ Pattern Matching เป็นการเปรียบเทียบ Packet ของ Signature และ Stateful Matching เป็นการเปรียบเทียบรูปแบบของกิจกรรมทั่วไป

๓.๒.๓.๓ (๒) การตรวจหาเหตุการณ์ผิดปกติ (Anomaly-Based Detection) เป็นการตรวจหารูปแบบการบุกรุกด้วยการวิเคราะห์พฤติกรรมหรือเหตุการณ์ที่เกิดขึ้นในระบบเครือข่าย โดยการเปรียบเทียบพฤติกรรมหรือเหตุการณ์ที่เข้ามาในเครือข่าย ณ เวลาขณะนั้น กับพฤติกรรมหรือเหตุการณ์ที่ปกติซึ่งจัดเก็บไว้ในฐานข้อมูลระบบ หากเปรียบเทียบแล้วไม่ตรงกันแสดงว่าพฤติกรรมหรือเหตุการณ์นั้นเป็นการบุกรุกก็จะแจ้งเตือนให้ผู้รับผิดชอบระบบทราบ

๓.๒.๓.๓ (๓) การวัดตามกฎ (Rule-Based Measure) เป็นวิธีการวัดโดยกำหนดพฤติกรรมหรือเหตุการณ์ปกติเป็นกฎไว้ แล้วนำพฤติกรรมหรือเหตุการณ์ที่เกิดขึ้นในเครือข่าย ณ เวลาในขณะนั้น มาเปรียบเทียบกับกฎ หากไม่ตรงกันแสดงว่าเป็นรูปแบบการโจมตี

๓.๒.๓.๔ คุณลักษณะของระบบตรวจจับการบุกรุก

๓.๒.๓.๔ (๑) ทำงานอยู่ตลอดเวลาได้เอง โดยไม่ต้องมีการควบคุมของผู้ดูแลระบบ และระบบต้องมีความน่าเชื่อถือที่เพียงพอที่จะทำงานในลักษณะอยู่เบื้องหลัง แต่ผู้ดูแลระบบต้องสามารถตรวจสอบการทำงานจากภายนอกได้

๓.๒.๓.๔ (๒) เป็นระบบที่เป็น Fault Tolerant หมายถึง ระบบยังคงสามารถทำงานต่อไปได้ในกรณีที่ระบบคอมพิวเตอร์เกิดปัญหาหรือมีข้อผิดพลาดเกิดขึ้นและไม่ต้องมีการสร้างฐานข้อมูลความรู้ (Knowledge-Base) ทุกครั้งที่เริ่มระบบ

๓.๒.๓.๔ (๓) มีความสามารถในการตรวจสอบตัวเองเพื่อไม่ให้ถูกลบ ทำลาย แก้ไข หรือถูกแทนที่ด้วยโปรแกรมอื่นได้

๓.๒.๓.๔ (๔) ส่งผลกระทบกันการทำงานของระบบคอมพิวเตอร์น้อยที่สุด

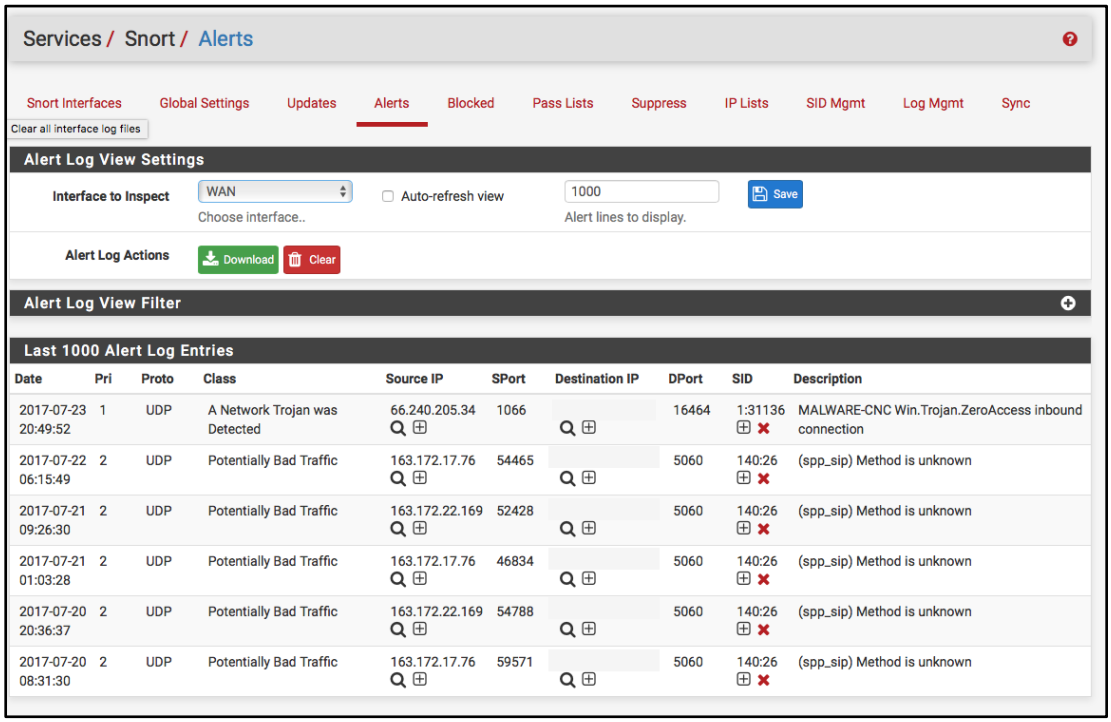
๓.๒.๓.๔ (๕) ตรวจสอบการทำงานที่ผิดไปจากรูปแบบการทำงานปกติได้

๓.๒.๓.๔ (๖) ปรับเปลี่ยนหรือแก้ไขให้เข้ากับระบบคอมพิวเตอร์ได้ง่าย เนื่องจากแต่ละระบบคอมพิวเตอร์จะมีรูปแบบการใช้งานและกลไกในการป้องกันที่ต่างกัน

๓.๒.๓.๔ (๗) ปรับการทำงานให้สอดคล้องกับการเปลี่ยนแปลงพฤติกรรมการใช้งานของระบบได้

๓.๒.๓.๔ (๘) มีความผิดพลาดในการทำงานน้อยที่สุด

๓.๒.๓.๕ ตัวอย่างเครื่องมือของระบบตรวจจับการบุกรุก Snort, OSSEC, Sguil และ Security Onion



ภาพที่ ๔๐ ตัวอย่างระบบ Snort เป็นซอฟต์แวร์ประเภท IDS/IPS

๓.๒.๓.๖ ข้อจำกัดของระบบตรวจจับการบุกรุก

๓.๒.๓.๖ (๑) ตรวจจับปัญหาร้ายแรงที่เพิ่มขึ้นเรื่อย ๆ

๓.๒.๓.๖ (๒) มีวิธีการบุกรุกใหม่ ๆ ถูกพัฒนาอยู่ตลอดเวลา

๓.๒.๓.๖ (๓) ต้องมีการอัพเดทหรือเพิ่มลายเซ็น (Signature) อยู่เสมอ

๓.๒.๓.๖ (๔) IDS มองหารูปแบบที่เป็นจุดอ่อนที่รู้อยู่แล้ว หรือการกระทำปกติ (Look for known)

๓.๒.๓.๖ (๕) มีการใช้เครื่องมือหรือเทคนิคต่าง ๆ ที่จะหลบหลีกการตรวจจับหรือมีการป่วนกระบวนการทำให้เกิดการแจ้งเตือนที่ผิดพลาดสูง

๓.๒.๔ Network Access Control

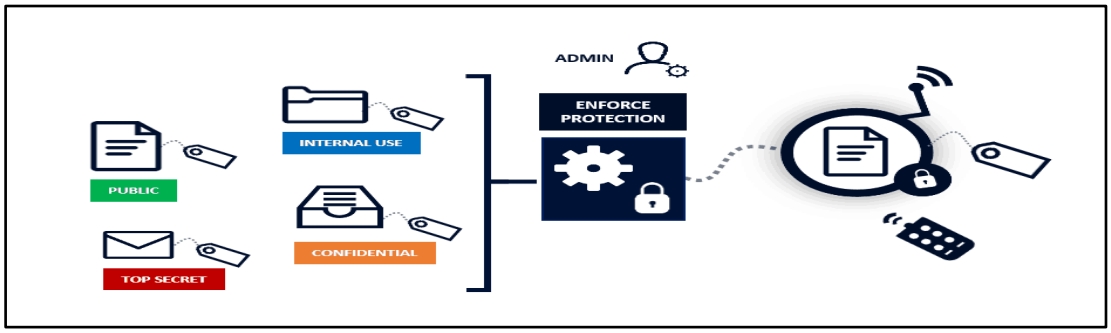
Network Access Control (NAC) เป็นอุปกรณ์ที่ทำหน้าที่ในการตรวจสอบและควบคุมผู้ใช้งานและเครื่องที่ใช้งานในระบบเครือข่าย เพื่อป้องกันภัยที่อาจจะเกิดขึ้นภายในระบบเครือข่าย เช่น ป้องกันผู้ใช้งานที่ไม่ได้รับอนุญาตมาใช้งานเครือข่ายและทรัพยากรในเครือข่าย ควบคุมผู้ใช้งานที่ได้รับอนุญาตให้ใช้งานเครือข่ายตามหน้าที่ที่รับผิดชอบเท่านั้น ตรวจสอบความพร้อมของเครื่อง

ก่อนอนุญาตให้ใช้งานเครือข่าย ได้แก่ ตรวจสอบโปรแกรม Antivirus, Personal Firewall โดยสามารถห้ามการใช้งานเครือข่ายในกรณีที่เครื่องตรวจสอบไม่ผ่าน และสามารถอนุญาตสำหรับเครื่องที่ไม่ผ่านการตรวจสอบให้ไปทำการติดตั้งโปรแกรมหรือ Patch เพื่อให้ผ่านการตรวจสอบ เป็นต้น ทั้งนี้ยังนำข้อมูลเหตุการณ์ต่าง ๆ ที่เกิดขึ้นในเครือข่าย นำมาวิเคราะห์หาพฤติกรรมที่เป็นการบุกรุกและรายงานสรุปเหตุการณ์ได้

๓.๒.๔.๑ ข้อจำกัดของระบบตรวจจับการบุกรุกความสำสำคัญของ NAC เป็นเทคโนโลยีที่กำลังได้รับความสนใจจากหลายองค์กร ความสามารถของ NAC ได้แก่ ความสามารถในการช่วยแบ่งเบาภาระขององค์กรในการจัดการปัญหาเกี่ยวกับการที่พนักงานภายในองค์กรนำเครื่องคอมพิวเตอร์ที่ไม่ได้รับอนุญาต เช่น คอมพิวเตอร์พกพา (Laptop หรือ Notebook) ส่วนบุคคลของพนักงานเข้ามาเชื่อมต่อกับระบบเครือข่ายภายในขององค์กร การกระทำดังกล่าวของพนักงานอาจทำให้ระบบเครือข่ายภายในองค์กรถูกบุกรุกผ่านทางเครื่องคอมพิวเตอร์ส่วนบุคคลของพนักงานได้ หากเครื่องดังกล่าวไม่มีความปลอดภัยเพียงพอซึ่ง NAC ถือว่าเป็นทางเลือกที่น่าสนใจอีกทางเลือกหนึ่งในการแก้ไขปัญหาตรงจุดนี้

๓.๒.๔.๒ หน้าที่ของ NAC คือการควบคุมสิทธิ์ในการเข้าถึงระบบเครือข่าย (Network Access Control) การที่จะควบคุมสิทธิ์ในการควบคุมการเข้าถึงระบบเครือข่ายได้นั้น เบื้องต้นอุปกรณ์ NAC จะต้องแยกแยะและรู้จักอุปกรณ์อื่น ๆ ในระบบเครือข่ายทั้งหมด ได้แก่ PC, Server, Printer, IP Phone, Switch, Router หรือ Access Point แล้วจึงค่อยทำการกำหนดสิทธิ์ต่าง ๆ ตามนโยบายความปลอดภัย เช่น การยืนยันตัวตน สิทธิ์ในการเข้าถึง Server และ Printer สิทธิ์ในการใช้งาน Protocol ต่าง ๆ หรือการบังคับลง Software และ Patch ต่าง ๆ กัน เป็นต้น โดยจำแนกได้ดังต่อไปนี้

๓.๒.๔.๒ (๑) Automatic Discovery and Classification การติดตั้งอุปกรณ์ NAC เข้าไปในระบบเครือข่าย อุปกรณ์ NAC จะช่วยค้นหาอุปกรณ์อื่น ๆ ทั้งหมดในระบบมาแสดงเป็นภาพรวมให้เห็นก่อน และค่อย ๆ ทำการจัดแบ่งประเภทอุปกรณ์ออกจากกัน ว่าเป็นคอมพิวเตอร์ติดตั้งระบบปฏิบัติการประเภทใด หรือเป็นอุปกรณ์เครือข่ายอื่น ๆ ในบางกรณี ผู้ดูแลระบบติดตั้งตัว NAC ไปเพื่อวัตถุประสงค์ทางด้าน Discovery เป็นหลัก เนื่องจากความหลากหลายของอุปกรณ์ เครือข่ายภายในองค์กร ผู้ใช้งานที่มีอุปกรณ์ส่วนตัวเข้ามาใช้งานมาก หรือมีอุปกรณ์เก่า ๆ ที่อยู่ในระบบตั้งแต่ผู้ดูแลระบบเข้ามาทำงาน ทำให้ผู้ดูแลระบบเห็นภาพรวมของระบบเครือข่ายโดยไม่ยึดติดกับยี่ห้อของอุปกรณ์ใด ๆ



ภาพที่ ๔๑ NAC

๓.๒.๔.๒ (๒) Identity-Based Policy Enforcement : สามารถบังคับใช้นโยบายความปลอดภัยต่าง ๆ ในลักษณะของ Identity-based ได้ โดยนำข้อมูลจากการค้นหาและจำแนกในข้อที่ ๑ มาบังคับใช้อุปกรณ์ประเภทไหนจะมีสิทธิ์เข้าถึงระบบเครือข่าย และอุปกรณ์ประเภทไหนจะต้องทำการยืนยันตัวตนด้วยวิธีการแบบใด เช่น Mac Authentication, 802.1X หรือ Web Authentication และจะยืนยันกับฐานข้อมูลใด เช่น Microsoft AD, LDAP, RADIUS, Novell หรือ Local Database เป็นต้น ในบางองค์กร อาจมีการกำหนดนโยบายแยกตามผู้ใช้งานตามแผนก โดยมีการดึงข้อมูลจาก AD หรือ LDAP มาช่วยจำแนก หรือให้อุปกรณ์ NAC จำแนกให้เองได้ โดยเฉพาะภายในองค์กรที่พนักงานมีการย้ายสถานที่ทำงานบ่อยครั้ง จนไม่สามารถ Fix IP หรือ VLAN ให้ผู้ใช้งานแต่ละคนได้ เพื่อให้ผู้ใช้งานแต่ละแผนกมีสิทธิ์ในการเข้าถึงข้อมูลที่แตกต่างกัน สำหรับกรณีของ Guest อาจมีความต้องการสำหรับ Guest Registration Page เพื่อให้สามารถลงทะเบียนด้วยตนเอง และรอรับการยืนยันจาก Admin

๓.๒.๔.๒ (๓) Network-Based Policy Enforcement : สามารถบังคับสิทธิ์ในการเข้าถึงระบบเครือข่ายของผู้ใช้งานรายบุคคลได้ เปรียบเสมือนการติดตั้ง Firewall ไว้ที่ด้านหน้าของเครื่อง PC และ Notebook แต่ละเครื่อง เพื่อให้สิทธิ์ในการเข้าถึงข้อมูลเป็นไปดังที่นโยบายกำหนดไว้ประเด็นหลัก ๆ ที่ผู้ดูแลระบบต้องพิจารณาก็คือ “วิธีการที่ใช้ในการควบคุมสิทธิ์ของ NAC แต่ละยี่ห้อ” ซึ่งแต่ละยี่ห้อเองก็มีวิธีการในการบังคับที่แตกต่างกันไป ไม่ว่าจะเป็นการใช้ Agent, SNMP, Switch Control, Firewall Control, 802.1X, Virtual Firewall หรือในกรณีที่เลวร้ายที่สุด อาจอนุญาตให้ NAC ทำ ARP Spoofing โจมตีทั้งระบบเครือข่ายพร้อม ๆ กันโดยไม่รู้ตัวก็เป็นได้

๓.๒.๔.๒ (๔) Application-Based Policy Enforcement : สามารถบังคับสิทธิ์การใช้งาน Application ของผู้ใช้งานในระบบได้ โดยการติดตั้ง Agent Software หรือการ Remote ผ่านทาง Administrator Account ของ Microsoft AD เพื่อบังคับให้มีการติดตั้งและใช้งาน Software ต่าง ๆ ที่จำเป็น เช่น Antivirus, PC Management หรือ OS Patch เป็นต้น และบังคับให้หยุดใช้งานโปรแกรมที่ผิดนโยบายขององค์กร เช่น การเล่น MSN ในเวลาทำงานและการโหลด BitTorrent เป็นต้น

๓.๒.๔.๒ (๕) IPS-Based Policy Enforcement : สามารถทำหน้าที่เป็น IPS เพื่อตรวจจับการโจมตีระบบเครือข่ายจากผู้ใช้งานแต่ละคนได้ ไม่ว่าจะเป็นการโจมตีโดยตั้งใจ หรือการโจมตีโดยไม่รู้ตัวผ่านทางไวรัสและเวิร์ม แล้วนำข้อมูลตรงนี้มาบังคับสิทธิ์ในการเข้าถึงระบบเครือข่ายที่เข้มข้นยิ่งขึ้น เช่น ห้ามใช้ Protocol อื่น ๆ นอกเหนือจาก HTTP หรือ ห้ามเข้าถึง Server ใด ๆ ในขณะที่ต้องสงสัยว่าอาจจะติดไวรัสหรือโจมตีระบบเครือข่าย เป็นต้น

๓.๒.๔.๒ (๖) Real Time Monitoring and Reporting : NAC ที่ดีจะต้องมีหน้าจอสำหรับทำการ Monitor แบบ Real Time เพื่อให้ผู้ดูแลระบบสามารถติดตามเหตุการณ์ที่เกิดขึ้นได้อย่างทันท่วงที รวมถึงสามารถสรุปเหตุการณ์ต่าง ๆ ที่เกิดขึ้นเพื่อนำไปวิเคราะห์ข้อมูลเพิ่มเติมได้

๓.๒.๔.๓ วัตถุประสงค์ของ NAC

๓.๒.๔.๓ (๑) การลดการโจมตีแบบ Zero-Day

๓.๒.๔.๓ (๒) การอนุญาตการรับรองความถูกต้องและการบัญชีของการเชื่อมต่อเครือข่าย

๓.๒.๔.๓ (๓) การเข้ารหัสการรับส่งข้อมูลไปยังเครือข่ายไร้สายและแบบใช้สายโดยใช้โปรโตคอลสำหรับ 802.1X เช่น EAP-TLS, EAP-PEAP หรือ EAP-MSCHAP เป็นต้น

๓.๒.๔.๓ (๔) การควบคุมตามบทบาทของผู้ใช้อุปกรณ์แอปพลิเคชันหรือการตรวจสอบความปลอดภัยหลังการโพสต์

๓.๒.๔.๓ (๕) การทำงานอัตโนมัติด้วยเครื่องมืออื่น ๆ เพื่อกำหนดบทบาทเครือข่ายตามข้อมูลอื่น ๆ

๓.๒.๔.๓ (๖) การบังคับใช้นโยบาย

๓.๒.๔.๓ (๗) การจัดการข้อมูลประจำตัวและการเข้าถึง

๓.๒.๔.๔ หลักการทำงานของ NAC จะทำการตรวจสอบควบคุมการลงทะเบียนเครื่องคอมพิวเตอร์ของผู้ที่ต้องการเข้าระบบว่าเป็นผู้ที่มีสิทธิ์ในการเข้าระบบหรือไม่ ทั้งที่เป็น PC แบบตั้งโต๊ะ และ PC ที่เป็นเครื่องแม่ข่าย รวมถึง Notebook และคอมพิวเตอร์พกพาขนาดเล็ก (Personal Digital Assistants) โดยใช้วิธีการ Authentication กับอุปกรณ์เครือข่ายที่นิยมใช้โปรโตคอล IEEE 802.1X อีกทั้ง มีการตรวจสอบเครื่องลูกข่ายว่าเป็นไปตามนโยบายความปลอดภัยขององค์กรหรือไม่ก่อนที่จะให้เครื่องลูกข่ายเข้าสู่ระบบ เช่น มีการตรวจ Anti-Virus Signature ว่ามีการ Update ล่าสุดหรือไม่ มีการตรวจสอบ Patch ของ Windows ว่าล่าสุดและเพียงพอหรือไม่ รวมทั้งตรวจสอบว่าเครื่องลูกข่ายมีการติดตั้ง Personal Firewall ที่เหมาะสมหรือไม่ เป็นต้น หากไม่เป็นไปตามนโยบายก็จะโยกเครื่องลูกข่ายนั้นไปยังเขตกักกัน (Quarantine Zone) หรือไม่ทำการอนุญาตให้เข้าระบบ จนกว่าเครื่องลูกข่ายจะมีการปรับปรุงให้ตรงตามนโยบายการรักษาความปลอดภัยทางคอมพิวเตอร์ขององค์กร

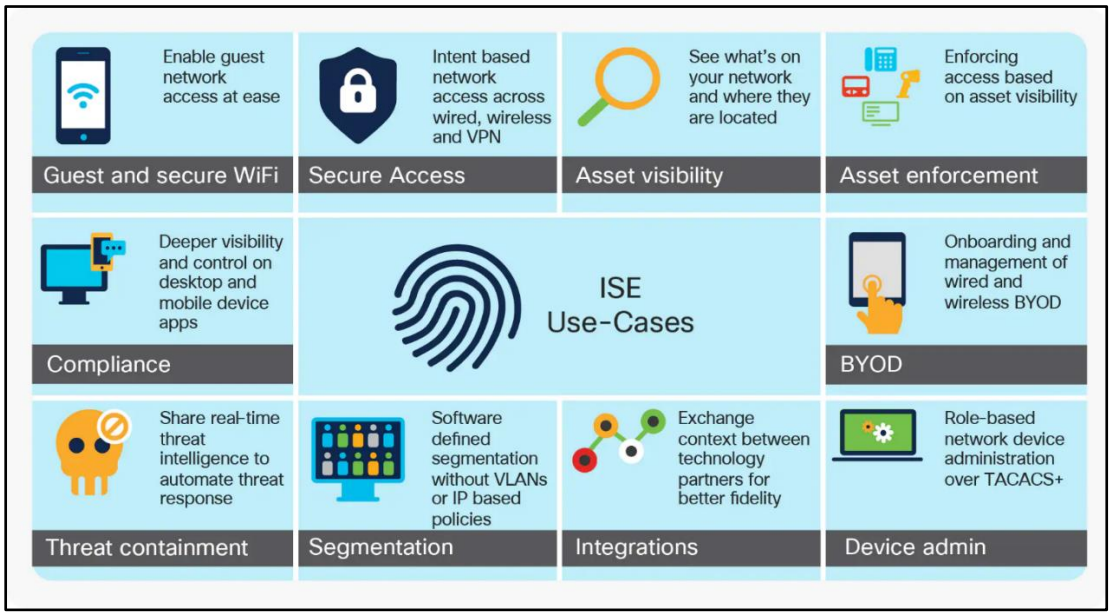
๓.๒.๔.๔ (๑) Pre-admission และ Post-admission ในการออกแบบ NAC โดยทั่วไปมีสองแบบ ขึ้นอยู่กับว่าจะมีการใช้นโยบายก่อนหรือหลังจากที่เครื่องสามารถเข้าถึงเครือข่ายได้ ในกรณีแรกเรียกว่า Pre-admission NAC เครื่องในเครือข่ายจะได้รับการตรวจสอบก่อนที่จะได้รับอนุญาตให้เข้าถึงเครือข่ายได้ NAC แบบ Pre-admission ส่วนใหญ่ใช้เพื่อป้องกันไคลเอนท์ที่ไม่ได้อัปเดต Signature ของไวรัสไม่ให้สามารถติดต่อกับเซิร์ฟเวอร์ที่มีข้อมูลความลับ ส่วน NAC แบบ Post-admission ใช้การบังคับโดยตัดสินใจจากการกระทำของผู้ใช้งาน หลังจากที่ผู้ใช้เหล่านี้สามารถเข้าถึงเครือข่ายได้แล้ว

๓.๒.๔.๔ (๒) Agent และ Agentless ความคิดพื้นฐานเบื้องหลังการทำงาน NAC คือการยอมให้เครือข่ายนั้นสามารถตัดสินใจเกี่ยวกับการควบคุมการเข้าถึงตามข้อมูลข่าวสารเกี่ยวกับระบบของผู้ใช้ ดังนั้น ข้อมูลเกี่ยวกับระบบของผู้ใช้เป็นการตัดสินใจที่สำคัญ ความแตกต่างที่สำคัญ คือ ความจำเป็นต้องใช้ซอฟต์แวร์ Agent เพื่อรายงานลักษณะของระบบปลายทาง หรือใช้เทคนิคการสแกน Network Inventory เพื่อให้รู้ถึงลักษณะเหล่านี้จากระยะไกล

๓.๒.๔.๔ (๓) Inline NAC เป็น NAC ที่มีการติดตั้งขวางเส้นทางการส่งข้อมูลในระบบเครือข่าย เช่นเดียวกับ Firewall และ IPS ซึ่งปัญหาที่มักจะพบคือ NAC ทำให้ระบบ

เครือข่ายทำงานช้าลง หรือเมื่ออุปกรณ์ NAC มีปัญหาแล้ว เครือข่ายต้องหยุดทำงาน ยกเว้นจะทำการติดตั้งแบบ Redundant ซึ่งมีค่าใช้จ่ายสูงมาก และอาจมีปัญหา เรื่องจำนวนพอร์ตที่ Core Switch ไม่พออีกด้วย

๓.๒.๔.๔ (๔) Out-of-Band NAC เป็น NAC ที่มีการติดตั้งในลักษณะที่ไม่ขวางเส้นทางการส่งข้อมูลในระบบเครือข่าย เพื่อให้ระบบเครือข่ายยังคงทำงานด้วยความเร็วปกติ ในขณะที่ทำการควบคุมสิทธิ์การเข้าถึงข้อมูลปัญหาที่เกิดขึ้นคือ Out-of-Band NAC นั้น ถูกสร้างขึ้นมาด้วยเทคโนโลยีที่หลากหลายมากตามแต่ละองค์กรจะเลือกใช้



ภาพที่ ๔๒ ISE Use – Cases

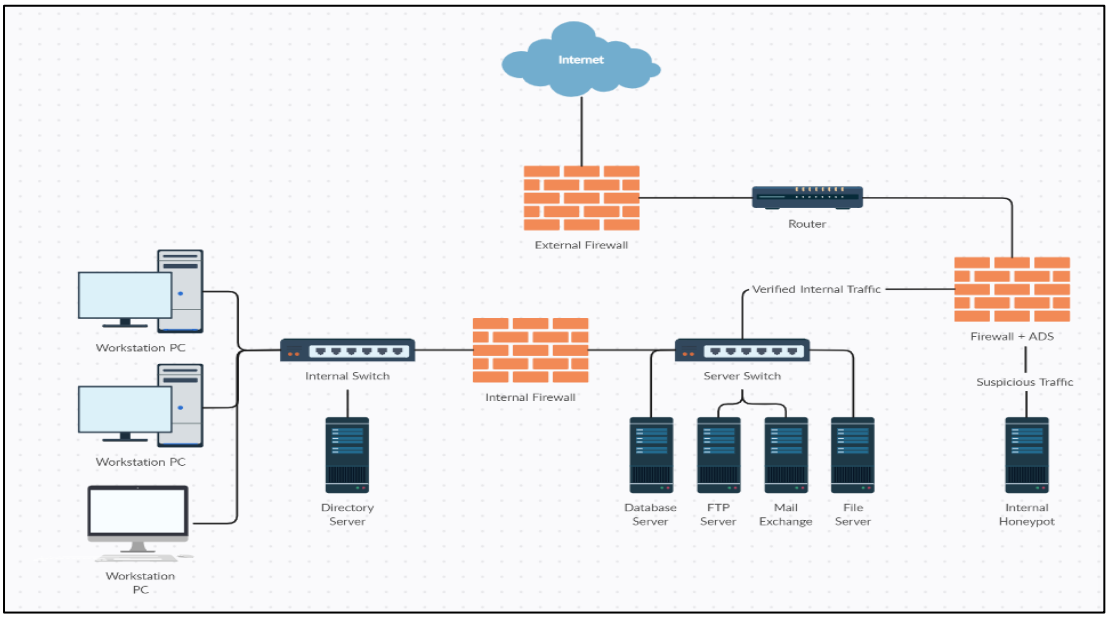
๓.๒.๕ Network Security Monitoring Tools เป็นเครื่องมือที่สำคัญสำหรับติดตามและเฝ้าระวังระบบเครือข่าย โดยนำข้อมูล Log ที่จัดเก็บมาวิเคราะห์และแสดงผลให้ผู้ดูแลระบบ รวมไปถึงแจ้งเตือนพฤติกรรมการใช้งานที่ผิดปกติที่ส่งผลกระทบกับองค์กร มีวัตถุประสงค์ ดังนี้

๓.๒.๕.๑ วัตถุประสงค์ของ Network Security Monitoring Tools

๓.๒.๕.๑ (๑) Availability ความต่อเนื่องของการให้บริการ ได้แก่ การ Monitor ดู Node หรืออุปกรณ์ รวมทั้ง Interface ต่าง ๆ ว่าสถานะเป็นอย่างไร (Up หรือ Down) การ Monitor จะต้องครอบคลุมไปถึง Node หรือ Interface เกิดการ Restart หรือ Reset อีกด้วย เนื่องจากการเกิด Restart หรือ Reset บ่อย เป็นสัญญาณเตือนระบบเครือข่าย หรือเครื่องนั้นกำลังเกิดปัญหา

๓.๒.๕.๑ (๒) สามารถแจ้งเตือนในกรณีที่เกิดความผิดพลาดประเมินความผิดพลาดของระบบในกรณีเกิดความผิดพลาดในอุปกรณ์เครือข่าย หรือสัญญาณอินเทอร์เน็ต เพื่อสามารถตรวจเช็ค แก้ไข และซ่อมแซมได้ทันที

๓.๒.๕.๑ (๓) สามารถตรวจสอบปริมาณการใช้งานทรัพยากรของเครือข่ายอีกทั้งยังต้องตั้งค่าในกรณีที่ปริมาณการใช้งาน เกินค่ากำหนด ซึ่งอาจนำไปสู่การทำงานที่ผิดพลาดของระบบเครือข่าย หรือประสิทธิภาพลดลงได้



ภาพที่ ๔๓ Network Security Monitoring tools

๓.๒.๕.๒ คุณสมบัติของ Network & Performance Monitoring

๓.๒.๕.๒ (๑) ควบคุมอุปกรณ์รักษาความมั่นคงปลอดภัยเพื่อให้มั่นใจได้ว่าอุปกรณ์เหล่านั้นทำงานได้อย่างถูกต้อง เช่น ฐานข้อมูลภัยคุกคามอัปเดตล่าสุด และระบบสำรองข้อมูลทำงานได้ตามปกติ IPS กำลังทำงานอยู่ เป็นต้น

๓.๒.๕.๒ (๒) ช่วยสนับสนุนด้านความมั่นคงปลอดภัย ในกรณีที่เกิดการโจมตีแบบ Zero-day ซึ่งทะลุผ่านระบบรักษาความมั่นคงปลอดภัยเข้ามาได้ อุปกรณ์ควรสามารถตรวจจับพฤติกรรมที่ผิดแปลกไปจากเดิม เช่น ปริมาณทราฟฟิคที่เพิ่มขึ้นจนผิดปกติ การใช้งาน Memory ที่เพิ่มสูงขึ้น หรือทราฟฟิกอีเมลแปลก ๆ เป็นต้น

๓.๒.๕.๒ (๓) ตรวจสอบการทำงานของระบบเครือข่ายอุปกรณ์ควรติดตามการทำงานของระบบเครือข่ายตลอดเวลา ไม่ว่าจะเป็นฮาร์ดแวร์ ซอฟต์แวร์ หรือข้อมูลที่วิ่งไปมาบนระบบ เพื่อช่วยป้องกันข้อมูลรั่วไหลสู่ภายนอกและนำข้อมูลที่ได้มาปรับปรุงระบบให้มีประสิทธิภาพดียิ่งขึ้น

๓.๒.๕.๒ (๔) ติดตามการใช้อุปกรณ์ IoT นอกจาก PC, Server และอุปกรณ์เครือข่ายแล้ว ควรสามารถติดตามอุปกรณ์ IoT เช่น อุปกรณ์พกพา กล้องวงจรปิด และอุปกรณ์พิสูจน์ตัวตน เป็นต้น เพื่อให้มั่นใจได้ว่าอุปกรณ์ทั้งหมดที่เชื่อมต่อกับระบบเครือข่ายทำงานได้อย่างถูกต้อง

๓.๒.๕.๒ (๕) เฝ้าระวังแบบรวมศูนย์ สามารถแสดงผลข้อมูลทั้งหมดบนระบบเครือข่ายได้แบบรวมศูนย์ เห็นถึงภาพรวม ตีความได้ง่าย และเป็นข้อมูลล่าสุด ณ เวลานั้น ๆ รวมไปถึงสามารถแสดงข้อมูลรายละเอียดเชิงลึกเมื่อต้องการได้

๓.๒.๕.๓ ตัวอย่างของ Network Security Monitoring tools

PRTG Network Monitor ซึ่งเป็น Software ที่สามารถเฝ้าระวัง ตรวจสอบ ควบคุม ดูแล จัดการระบบเครือข่าย รวมไปถึงการแจ้งเตือน โดยใช้เทคโนโลยีหลายอย่างในการตรวจสอบ เช่น SNMP, WMI, SSH, Flows/Packet Sniffing, HTTP requests, REST APIs, Pings, SQL เป็นต้น โดยคุณสมบัติเด่นของ PRTG Network Monitoring ประกอบด้วย

๓.๒.๕.๓ (๑) สามารถมอนิเตอร์การใช้งานอุปกรณ์ Windows, Mac OS X, Linux และ Unix ผ่าน SNMP, WMI, Flow Monitoring และ Packet Sniffing โดยไม่จำเป็นต้องลง Agent

๓.๒.๕.๓ (๒) มี Sensor พร้อมให้บริการมากกว่า ๒๐๐ รายการสำหรับติดตามการใช้เว็บไซต์ อีเมล แอปพลิเคชัน ฐานข้อมูล อุปกรณ์ฮาร์ดแวร์ และการใช้งานแบบ Virtualization ไม่ว่าจะเป็น Bandwidth, Usage, Activity, Uptime, Downtime และ SLA ได้อย่างครอบคลุม

๓.๒.๕.๓ (๓) ติดตามและเฝ้าระวังการใช้ระบบเครือข่าย LAN และ WAN ของทั้งสำนักงานใหญ่และสำนักงานสาขาได้แบบรวมศูนย์ โดยไม่จำเป็นต้องเสียค่าใช้จ่ายเพิ่มเติม

๓.๒.๕.๓ (๔) จัดทำ Network Diagram แบบ Interactive พร้อมแสดงผลข้อมูลแบบเรียลไทม์

๓.๒.๕.๓ (๕) จัดเก็บ Log แบบ RAW ซึ่งเหมาะสำหรับนำไปวิเคราะห์ข้อมูลในอนาคตมากกว่าการเก็บข้อมูลบนฐานข้อมูล SQL

๓.๒.๕.๓ (๖) รองรับการทำ Failover Clustering ซึ่งช่วยให้มั่นใจได้ว่าสามารถใช้งาน PRTG ได้ตลอดเวลา

๓.๒.๕.๓ (๗) ติดตั้งและบริหารจัดการได้ง่ายภายในไม่กี่นาที หน้า Dashboard มีความสวยงาม ปรับแต่งได้หลากหลายรูปแบบ และสามารถเลือกดูรายละเอียดเชิงลึกได้ทันที

๓.๒.๕.๓ (๘) จัดทำรายงานได้หลากหลายรูปแบบ รวมไปถึงจัดเก็บ Event Log แล้วส่งต่อไปยังอุปกรณ์ SIEM เพื่อวิเคราะห์ข้อมูล Security Intelligence ต่อได้

ภาพที่ ๔๔ Vulnerability Assessment (VA)

๓.๒.๖ Vulnerability Assessment (VA) คือ การตรวจสอบอย่างเป็นระบบในเรื่องของการหาช่องโหว่ทางด้านความความปลอดภัย โดยจะใช้การประเมินว่าระบบจะสามารถโดนเจาะผ่านช่องโหว่ทางไหน หรือด้วยการโจมตีลักษณะใดได้บ้าง รูปแบบของการทำ VA Scan ดังนี้

ภาพที่ ๔๕ Vulnerability Identification

๓.๒.๖.๑ Host Assessment คือ การประเมินความเสี่ยงในส่วนของ Server ที่มีความสำคัญ ซึ่งอาจจะเป็นเป้าหมายในการโจมตีได้หากไม่ได้รับการทดสอบอย่างเพียงพอ หรือไม่ได้ใช้ OS ที่มาจาก Image ที่เคยมีการทดสอบเรื่องของ VA มาแล้ว

๓.๒.๖.๒ Network and Wireless Assessment คือ การประเมินความเสี่ยงโดยมีการกำหนด Policy และนำไปปฏิบัติจริงเพื่อป้องกันไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาตทั้งใน Private Network หรือ Public Network ที่สามารถเข้าถึงระบบได้

๓.๒.๖.๓ Database Assessment คือ การประเมินความเสี่ยงในเรื่องของ Database หรือระบบที่เกี่ยวข้องกับข้อมูล เช่น Big Data จะใช้การตรวจสอบจาก Database ปลอม หรือ Dev/Test Server ที่ความปลอดภัยหละหลวม หลังจากนั้นจะทำการจัดลำดับความสำคัญของข้อมูล ใน Infrastructure ขององค์กรให้ เป็นต้น

๓.๒.๖.๔ Application Scans คือ วิธีการระบุช่องโหว่ทางด้านความปลอดภัยใน Web Application และ Source Code โดยการ Scan แบบอัตโนมัติที่ Front-end หรือไม่ก็วิเคราะห์ที่ Source Code

๓.๒.๖.๕ ขั้นตอนการทำ VA Scan ๔ ขั้นตอน ดังนี้

ภาพที่ ๔๖ ขั้นตอนการทำ VA Scan

๓.๒.๖.๖ การระบุช่องโหว่ โดยใช้วิธีทดสอบ จุดประสงค์ของขั้นตอนนี้ คือ การเตรียมรายการของช่องโหว่ใน Application ผู้ที่วิเคราะห์จะทำการทดสอบความแข็งแรงของระบบ Security ของ Application, Server หรือระบบอื่น ๆ โดยใช้เครื่องมือในการ Scan ระบบให้โดยอัตโนมัติ หรือทดสอบหรือประเมินด้วยตนเอง ซึ่งต้องใช้ข้อมูลจากการประกาศของ Vendor ที่มีการเก็บ Vulnerability Database ไว้ เพื่อช่วยให้ง่ายต่อการระบุช่องโหว่ที่เคยมีการเกิดขึ้นมาแล้ว

๓.๒.๖.๗ การวิเคราะห์ช่องโหว่และภัยคุกคาม จุดประสงค์ของขั้นตอนนี้ คือ การหาสาเหตุหรือต้นตอที่เจอช่องโหว่มาจากข้อที่ ๑ ซึ่งขั้นตอนนี้รวมไปถึงการระบุรายละเอียดของการทำงานของระบบว่ามีการตอบสนองต่อช่องโหว่อย่างไร และสาเหตุของการเกิดช่องโหว่ เช่น ปัญหานี้อาจเกิด

จากการใช้งาน Software ที่เป็น Open Source ที่ใช้ Library Version เก่า ที่นี้เราจะสามารถเลื่อนขั้นตอนไปสู่การแก้ไขได้โดยการ Update Library ให้เป็น Version ใหม่ เป็นต้น

๓.๒.๖.๘ การประเมินความเสี่ยง จุดประสงค์ของขั้นตอนนี้คือ การจัดลำดับความสำคัญของช่องโหว่ โดยจะทำการระบุเป็น Rank หรือ Score ว่าช่องโหว่ไหนร้ายแรงกว่ากัน โดยอ้างอิงจากความเสี่ยงและความเสียหายที่อาจจะเกิดขึ้นเมื่อช่องโหว่ถูกโจมตี

๓.๒.๖.๙ การแก้ไข จุดประสงค์ของขั้นตอนสุดท้ายนี้คือ การอุดช่องโหว่ โดยส่วนใหญ่จะเป็นการร่วมมือกันระหว่างทีมงานที่ดูแลเรื่อง Security กับทีม Operation ซึ่งเป็นผู้ที่สามารถบอกได้ว่าการอุดช่องโหว่แบบใด ระดับไหนจะมีประสิทธิภาพสูงสุดโดยที่ไม่กระทบกับระบบปัจจุบันหรืออาจจะกระทบน้อยลง

๓.๒.๗ โปรแกรมป้องกันไวรัสหรือ Antivirus เป็นโปรแกรมที่สร้างขึ้นเพื่อตรวจจับ ป้องกันและกำจัดโปรแกรมคุกคามทางคอมพิวเตอร์หรือมัลแวร์ซึ่งหมายถึง ไวรัส เวิร์ม โทรจัน สปายแวร์ แอดแวร์และซอฟต์แวร์คุกคามประเภทอื่น ๆ

๓.๒.๗.๑ ประเภทของโปรแกรมป้องกันไวรัส มีดังนี้

๓.๒.๗.๑ (๑) แอนติไวรัส (Anti-Virus) เป็นโปรแกรมป้องกันไวรัสทั่ว ๆ ไป จะค้นหาและทำลายไวรัสในคอมพิวเตอร์

๓.๒.๗.๑ (๒) แอนติสปายแวร์ (Anti-Spyware) เป็นโปรแกรมป้องกันการโจรกรรมข้อมูล จากไวรัสสปายแวร์ รวมถึงการกำจัด Adware ซึ่งเป็น Pop up โฆษณาอีกด้วย

๓.๒.๗.๑ (๓) โปรแกรมป้องกันไวรัสจะค้นหา ตรวจสอบ และทำลายไวรัสที่ไฟล์โดยตรง แต่ทุก ๆ ห้วงเวลาจะมีไวรัสชนิดใหม่เกิดขึ้นเสมอ ทำให้ต้องอัปเดตโปรแกรมป้องกันไวรัสเพื่อให้คอมพิวเตอร์ปลอดภัย ซึ่งโปรแกรมป้องกันไวรัสจะมีหลายรูปแบบและหลายผลิตภัณฑ์ แต่ละผลิตภัณฑ์จะมีการอัปเดตและวิธีการป้องกันไม่เหมือนกัน แต่ภายในคอมพิวเตอร์เครื่องเดียวไม่ควรมีโปรแกรมป้องกันไวรัส ๒ โปรแกรมเพราะจะทำให้โปรแกรมขัดแย้งกันเองจนไม่สามารถใช้งานได้

๓.๒.๗.๒ การทำงานของโปรแกรมป้องกันไวรัส

๓.๒.๗.๒ (๑) ตรวจสอบ ไวรัสซิกเนเจอร์ คือสัญลักษณ์ของไวรัส ซึ่งไวรัสแต่ละตัวจะมีสัญลักษณ์ที่แตกต่างกันออกไป เปรียบเหมือนลายเซ็นของคนทั่วไปที่ล้วนแตกต่างกันออกไป โดยหลักการทำงานของโปรแกรมป้องกันไวรัส จะมีการตรวจสอบไฟล์ว่ามีรหัสเหมือนกับไวรัสซิกเนเจอร์หรือไม่ ซึ่งหากใช่นั้นหมายถึงว่า ไฟล์ตัวนั้นคือไวรัส ดังนั้นโปรแกรมป้องกันไวรัส จึงควรต้องหมั่นอัปเดตอยู่เป็นประจำ เพื่อให้การป้องกันไวรัส เป็นไปได้อย่างทั่วถึง ซึ่งวิธีนี้เป็นวิธีที่ใช้กันแพร่หลายในปัจจุบัน

๓.๒.๗.๒ (๒) ตรวจสอบการเปลี่ยนแปลงของข้อมูล เป็นการตรวจหาค่าพิเศษที่เรียกว่า Checksum ของไฟล์ โดยหากเกิดการเปลี่ยนแปลงในตัวไฟล์ ซึ่งอาจเกิดจากไวรัส ค่านี้ก็จะเปลี่ยนแปลง ข้อดีคือ จะตรวจจับไวรัสชนิดใหม่ ๆ ได้ ปัญหาคือต้องแน่ใจว่าตัวเครื่องนั้น ไม่มีการติดไวรัส

๓.๒.๗.๒ (๓) ตรวจสอบการกระทำแปลกปลอมคอยตรวจสอบการกระทำที่แปลกปลอม จากไวรัสต่าง ๆ เช่น พยายามทำลาย เปลี่ยนแปลง หรือแก้ไขข้อมูลระบบโดยไม่ได้รับอนุญาต พยายามจดตัวเองในระบบรูต พยายามดาวน์โหลด/อัปโหลดข้อมูลและไฟล์ต่าง ๆ เป็นต้น

๓.๒.๗.๒ (๔) ตรวจสอบการกระทำ เป็นวิธีตรวจจับไวรัสโดยสร้าง Virtual Machine มีจุดอ่อนด้านความปลอดภัยจำนวนมาก เมื่อมีการรันโปรแกรมขึ้นมา ตัวโปรแกรมตรวจจับไวรัสจะตรวจสอบการกระทำหากมีการกระทำที่อาจเป็นอันตราย เช่น พยายามเขียนข้อมูลลงบนบูตเซกเตอร์ก็จะแจ้งไปยังผู้ใช้ หากว่าสิ่งที่ผู้ใช้กำลังทำไม่เกี่ยวกับสิ่งที่แจ้ง เช่น กำลังเล่นเกมอยู่แต่มีความพยายามเขียนข้อมูลลงบูตเซกเตอร์ ก็สามารถหยุดการทำงานนั้นลงได้ เป็นต้น

บทที่ ๔ หน่วยงานที่เกี่ยวข้อง การแจ้งเตือน การตอบสนองภัยคุกคาม และการสร้างความตระหนักรู้

การดำเนินการรักษาความปลอดภัยต่อระบบสารสนเทศของกองทัพอากาศ มีความจำเป็นต้องกำหนดหลักการและมาตรการป้องกัน เพื่อรักษาไว้ซึ่งคุณสมบัติที่มั่นคงและปลอดภัยต่อระบบสารสนเทศ เพื่อให้การดำเนินงานในการรักษาความมั่งคงปลอดภัยระบบสารสนเทศของกองทัพอากาศเป็นไปอย่างมีประสิทธิภาพ จึงมีการแบ่งมอบบทบาทและหน้าที่ความรับผิดชอบให้กับหน่วยงานที่เกี่ยวข้อง ดังนี้

๔.๑ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

๔.๑.๑ ภารกิจ มีหน้าที่พิจารณา เสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับการ พัฒนาและดำเนินการด้านระบบบัญชาการและควบคุมข่าย เครือข่ายเทคโนโลยีสารสนเทศและการสงครามสารสนเทศ การสื่อสารอิเล็กทรอนิกส์และการสงครามอิเล็กทรอนิกส์ กับมีหน้าที่จัดการความรู้ ควบคุม ประเมินผล และตรวจตรากิจการด้านสารสนเทศและสงครามอิเล็กทรอนิกส์ มีเจ้ากรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศเป็นผู้บังคับบัญชารับผิดชอบ

๔.๑.๒ การแจ้งเตือน

๔.๑.๒.๑ ประเมินความมั่นคงปลอดภัยของระบบสารสนเทศและดำเนินการกับสารสนเทศเพื่อระบุและแจ้งเตือนภัยที่จะเกิดกับระบบสารสนเทศของกองทัพอากาศ

๔.๑.๒.๒ แจ้งผลการตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศ (Information System Security Audit) รวมทั้งพิจารณาให้คำแนะนำ ติดตาม และประเมินผลตามนโยบายและระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓

๔.๑.๓ การตอบสนองภัยคุกคาม

๔.๑.๓.๑ พัฒนาหลักการ และกระบวนการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๔.๑.๓.๒ ให้การสนับสนุนระบบรวมถึงอุปกรณ์ที่เกี่ยวข้องกับการปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพอากาศ และส่งเสริมความร่วมมือกับหน่วยงานภายนอกที่เกี่ยวข้อง

๔.๑.๓.๓ รับรองการติดตั้งซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้ายบนเครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์แบบพกพา (Notebook)

๔.๑.๔ การสร้างความตระหนักรู้

๔.๑.๔.๑ สนับสนุนและส่งเสริมให้มีการศึกษาหลักสูตรการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ อย่างต่อเนื่อง

๔.๑.๔.๒ ดำเนินการฝึกอบรม สัมมนาและดูงาน เกี่ยวกับงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๔.๒ ศูนย์ไซเบอร์กองทัพอากาศ

๔.๒.๑ ภารกิจ มีหน้าที่ วางแผน เตรียมการ ประสานงาน ควบคุม กำกับการ พัฒนาและดำเนินการด้านไซเบอร์ของกองทัพอากาศ มีผู้อำนวยการ ศูนย์ไซเบอร์กองทัพอากาศ เป็นผู้บังคับบัญชารับผิดชอบ

๔.๒.๒ การแจ้งเตือน

๔.๒.๒.๑ เฝ้าระวังสถานการณ์ความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ โดยต้องมีการประเมิน และพิจารณาว่าเหตุการณ์ที่เกิดขึ้นเป็นสถานการณ์ที่ก่อให้เกิดความไม่มั่นคงปลอดภัย เพื่อดำเนินการแจ้งเตือนไปยังหน่วยงานที่เกี่ยวข้อง

๔.๒.๒.๒ แจ้งเตือนเหตุการณ์ ข่าวสารทางด้านไซเบอร์แก่ข้าราชการกองทัพอากาศผ่านช่องทางจดหมายอิเล็กทรอนิกส์กองทัพอากาศ (E-mail)

๔.๒.๓ การตอบสนองภัยคุกคาม

๔.๒.๓.๑ ดำเนินการร่วมกับภายนอกตอบสนองต่อเหตุการณ์ที่เป็นสถานการณ์ที่กระทบต่อความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์

๔.๒.๓.๒ ดำเนินการกู้คืนระบบสารสนเทศ เพื่อสนับสนุนการรับมือเหตุการณ์ทางไซเบอร์และการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล

๔.๒.๔ การสร้างความตระหนักรู้

๔.๒.๔.๑ ดำเนินการเกี่ยวกับการศึกษา ฝึกอบรม การวิจัยและพัฒนาด้านไซเบอร์ รวมทั้งให้การสนับสนุนการปฏิบัติการด้านไซเบอร์ให้แก่ข้าราชการกองทัพอากาศ

๔.๒.๔.๒ ดำเนินการจัดทำการทดสอบความตระหนักรู้ด้านไซเบอร์กำลังพลกองทัพอากาศตามวงรอบในแต่ละปีงบประมาณ

๔.๒.๔.๓ เผยแพร่ข้อมูลข่าวสาร ให้ความรู้ คำแนะนำ การแจ้งเตือนภัยทางด้านไซเบอร์แก่ข้าราชการกองทัพอากาศผ่านช่องทางจดหมายอิเล็กทรอนิกส์กองทัพอากาศ

(E-mail)และแจ้งเตือนภัยทางด้านไซเบอร์แก่ข้าราชการกองทัพอากาศผ่านช่องทางแพลตฟอร์มโซเชียลมีเดีย เช่น YouTube, Facebook และ Instagram เป็นต้น

๔.๓ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ

๔.๓.๑ ภารกิจ มีหน้าที่ วางแผนการปฏิบัติ อำนวยการ ประสานงาน ติดตาม กำกับการ พัฒนา และดำเนินการเกี่ยวกับกิจการสื่อสารอิเล็กทรอนิกส์ กิจการกระจายเสียงและกิจการโทรทัศน์ มาตรวิทยา และการพัสดุสื่อสารอิเล็กทรอนิกส์ กับมีหน้าที่จัดการความรู้ ควบคุม ประเมินผล และตรวจตรากิจการในสายวิทยาการด้านสื่อสารอิเล็กทรอนิกส์

๔.๓.๒ การแจ้งเตือน

๔.๓.๒.๑ รายงานผลการประเมินจากการตรวจตรากิจการในสายวิทยาการด้านระบบและอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศและไซเบอร์

๔.๓.๒.๒ รายงานสถานภาพพัสดุสื่อสารอิเล็กทรอนิกส์ ให้เป็นไปตามวงรอบของการประเมิน

๔.๓.๓ การตอบสนองภัยคุกคาม

ให้การสนับสนุนต่อเหตุการณ์ที่ตรวจพบหรือได้รับรายงาน โดยประสานหน่วยเกี่ยวข้องกับเหตุการณ์ ให้มีการสนับสนุนการปฏิบัติเป็นไปด้วยความเรียบร้อย

๔.๓.๔ การสร้างความตระหนักรู้

ดำเนินการสร้างองค์ความรู้ บริหารการฝึกและศึกษา เพื่อสนับสนุนการสร้างความปลอดภัยต่อระบบสารสนเทศและไซเบอร์

๔.๔ หน่วยขึ้นตรงกองทัพอากาศ

โดยมีการแต่งตั้งนายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๔.๔.๑ ภารกิจหน้าที่รับผิดชอบ ดำเนินการให้เป็นไปตามระเบียบและจัดทำมาตรการการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๔.๔.๒ การแจ้งเตือน

๔.๔.๒.๑ รายงานเหตุละเมิดความมั่นคงปลอดภัย หรือการกระทำที่ไม่เหมาะสมที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในหน่วยงาน

๔.๔.๒.๒ รายงานการทำงานที่ผิดปกติ ข้อผิดพลาดหรือช่องโหว่ของซอฟต์แวร์ที่ตรวจพบ

๔.๔.๒.๓ รายงานเหตุละเมิดความมั่นคงปลอดภัยหรือช่องโหว่

๔.๔.๒.๔ บันทึกรายละเอียดการเปลี่ยนแปลง แก้ไขที่สำคัญและแจ้งให้หน่วยงานที่เกี่ยวข้องทราบ กรณีที่มีการเปลี่ยนแปลงแก้ไขเครือข่าย

๔.๔.๓ การตอบสนองภัยคุกคาม

๔.๔.๓.๑ รายงานขั้นต้นต่อ ศูนย์ไซเบอร์กองทัพอากาศ เพื่อการค้นหาและตรวจพิสูจน์หลักฐานทางดิจิทัล (Digital Forensic)

๔.๔.๓.๒ รายงานต่อกรมข่าวทหารอากาศ หากพบว่าเป็นการละเมิดความมั่นคงปลอดภัยต่อระบบสารสนเทศที่มีชั้นความลับ เพื่อดำเนินการด้านการรักษาความปลอดภัย

๔.๔.๓.๓ ระงับการใช้งาน แก้ไข หรือยกเลิกระบบสารสนเทศที่สงสัยว่าถูกละเมิด เพื่อลดความเสียหายเบื้องต้น

๔.๔.๓.๔ สำรวจความเสียหายที่เกิดขึ้น ให้ตรวจสอบสาเหตุและช่องโหว่ หรือข้อบกพร่องที่ก่อให้เกิดการละเมิดโดยให้มีผู้แทนจาก ศูนย์ไซเบอร์กองทัพอากาศและกรมข่าวทหารอากาศร่วมในการตรวจสอบสาเหตุด้วย

๔.๔.๓.๕ รายงานเหตุการณ์ที่เกิดขึ้นให้ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศทราบ พร้อมทั้งแนวทางป้องกันมิให้เกิดเหตุซ้ำ

๔.๔.๓.๖ กรณีปรากฏหลักฐาน หรือสงสัยว่าระบบสารสนเทศถูกจารกรรม ให้รายงานกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศทราบ เพื่อแก้ไขโดยเร็วที่สุด

๔.๔.๓.๗ จัดทำแผนเตรียมรับสถานการณ์ฉุกเฉินต่าง ๆ เช่น แผนป้องกันอัคคีภัยของระบบสารสนเทศ และแผนเผชิญเหตุ (Contingency Plan) เป็นต้น

๔.๔.๓.๘ จัดทำคู่มือและขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน ต้องมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่ายที่สนับสนุนความมั่นคงปลอดภัย

๔.๔.๓.๙ สำรองข้อมูลการปฏิบัติภารกิจของหน่วย ให้สามารถนำกลับมาใช้ได้ในภายหลัง ในกรณีที่เกิดเหตุต่าง ๆ ที่ทำให้ข้อมูลสูญหายหรือถูกทำลาย เช่น ภัยจากการโจมตีทางไซเบอร์ ระบบล้มเหลว ภัยจากธรรมชาติ เป็นต้น

๔.๔.๓.๑๐ การสร้างความตระหนักรู้ จัดการฝึกอบรม สัมมนาและดูงานเกี่ยวกับงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ให้กับข้าราชการภายในหน่วย

นิยามศัพท์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์

กระบวนการในการป้องกันภัยคุกคามทางไซเบอร์นั้นเป็นกระบวนการที่กว้างและมีปรับปรุงอยู่เสมอเนื่องจากการโจมตีทางไซเบอร์มีการอุบัติขึ้นใหม่อยู่เป็นตลอดเวลา ซึ่งทำให้มีความจำเป็นจะต้องมีการศึกษาค้นคว้าและพัฒนากระบวนการในการป้องกันภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง เพื่อให้ทันต่อสถานการณ์ โดยจะมีคำนิยามศัพท์ที่เกี่ยวข้องพอสังเขป ดังนี้

(A)

Anonymous Website	เว็บไซต์ที่มีการปกปิดตนเองหรือไม่น่าไว้วางใจ
Asset	ข้อมูล ระบบข้อมูล ระบบคอมพิวเตอร์ ระบบเครือข่าย และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน
Attack	การโจมตีด้านความมั่นคงปลอดภัยด้านสารสนเทศและความมั่นคงปลอดภัยไซเบอร์
Availability	การจัดทำให้ทรัพย์สินสารสนเทศสามารถทำงานเข้าถึงหรือใช้งานได้ในเวลาที่ต้องการ

(B)

Biometrics	การนำลักษณะทางและลักษณะทางพฤติกรรมของบุคคลมาผสมผสานเข้ากับเทคโนโลยีเพื่อการระบุตัวตน หรือการพิสูจน์ตัวตน

Bit	หน่วยที่เล็กที่สุดของข้อมูลดิจิทัล มีได้ทั้งหมด ๒ ค่าคือ 1 (หนึ่ง) และ 0 (ศูนย์) สามารถนำมาประกอบกันเป็นชุดข้อมูลที่ใหญ่ขึ้นได้
	(C)
Certificate	ใบรับรอง ข้อมูลอิเล็กทรอนิกส์หรือการบันทึกอื่นใดซึ่งยืนยันความเชื่อมโยง ระหว่างเจ้าของลายมือชื่อกับข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์
Computer Forensics	การดำเนินการที่เกี่ยวข้องกับการตรวจสอบอาชญากรรมทางไซเบอร์ที่เกี่ยวข้องกับระบบคอมพิวเตอร์ โดยการใช้วิธีการเก็บรวบรวม ประมวลผล วิเคราะห์ข้อมูลหลักฐาน และให้เป็นที่ยอมรับในการดำเนินการทางกฎหมายในชั้นศาล
Confidentiality	การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต
Combat Information System (CIS)	ระบบสารสนเทศเพื่อการยุทธของกองทัพอากาศ
Computer Security incident Response Team (CSIRT)	ศูนย์ประสานการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ที่สามารถรับมือและแก้ไขเหตุภัยคุกคาม
Cipher Text	ข้อความเข้ารหัสลับ ข้อความที่เป็นผลลัพธ์จากกระบวนการเข้ารหัสลับที่ได้จาก ข้อมูลต้นฉบับ Plain Text
Critical Information Infrastructure (CII)	หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางระบบสารสนเทศ
Cyber Threats	การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมพึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง
Cyber Crime	การกระทำที่ละเมิดกฎหมาย โดยเกี่ยวข้องกับระบบคอมพิวเตอร์ หรือแอปพลิเคชันที่ใช้งาน
Cyber Criminals	บุคคลหรือกลุ่มบุคคลผู้ก่ออาชญากรรมบนโลกออนไลน์โดยใช้เทคนิควิธีต่าง ๆ ในการก่ออาชญากรรมไซเบอร์เพื่อใช้ในการโจมตีเหยื่อ

Cyber Security	มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกันรับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ
Cyber	ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ตหรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียม และระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป
	(D)
Decryption	การถอดรหัสลับ กระบวนการย้อนกลับของการเข้ารหัสที่เมื่อกระทำกับข้อมูลต้นฉบับ Cipher Text จะได้ผลลัพธ์เป็น Plain Text
Demilitarized Zone (DMZ)	เขตปลอดทหาร เขตโซนเครือข่ายที่อนุญาตให้ อุปกรณ์ภายในเครือข่ายสามารถติดต่อกับอินเทอร์เน็ต
Digital Evidence	หลักฐานดิจิทัล เป็นข้อมูลที่สามารถใช้เพื่อพิสูจน์ โดยมีการจัดเก็บหรือส่งผ่านในรูปแบบดิจิทัล
	(E)
Encryption	การเข้ารหัสลับ กระบวนการเปลี่ยนแปลงข้อมูลไปอยู่ในลักษณะที่ซ่อนข้อมูลจริง เพื่อปกปิดข้อมูลจากบุคคลอื่น จากข้อมูลต้นฉบับ Plain Text จะได้ผลลัพธ์เป็น Cipher Text
Evasion IDS	การหลบเลี่ยงระบบตรวจจับการบุกรุกเครือข่าย
Event Source	แหล่งที่มาของกิจกรรม หมายถึง คอมพิวเตอร์หรืออุปกรณ์ที่เป็น แหล่งกำเนิดของกิจกรรมในข้อมูลกิจกรรม
External Threats	การคุกคามและการโจมตีจากภายนอกองค์กร
Exploit	การนำช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศของทรัพย์สินสารสนเทศ มาใช้ในการเจาะระบบ สารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายขององค์กร รวมถึงการนำซอฟต์แวร์ที่เป็นอันตรายมาใช้งาน เช่น ซอฟต์แวร์ที่มีมัลแวร์ และซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ เป็นต้น
	(F)

Firewall	ซอฟต์แวร์ หรือฮาร์ดแวร์ที่สำหรับป้องกันเครือข่ายจากการบุกรุกของผู้ไม่หวังดี หรือชุดคำสั่งที่อาจก่อให้เกิดความเสียหายต่อระบบและเครือข่ายได้
Forensic Artifact	ข้อมูลใด ๆ ที่อยู่ในสื่อบันทึก หรือร่องรอยทางกายภาพใด ๆ ที่เกิดจากการปฏิสัมพันธ์ระหว่างสิ่งสองสิ่งและสามารถใช้ในการประกอบการทำนิติวิทยาศาสตร์ เพื่อพิสูจน์ข้อเท็จจริงหรือหาความกระจ่างให้กับเรื่องที่กำลังสนใจอยู่ได้
	(H)
Honeypot	การจัดทำระบบจำลองที่คล้ายกับระบบหรือเครื่องเซิร์ฟเวอร์จริง เพื่อหลอกล่อให้ผู้บุกรุกเข้าใจว่าระบบจำลองนี้เป็นระบบเป้าหมายของผู้ไม่หวังดี
	(I)
Incident	อุบัติการณ์ สถานการณ์ที่อาจทำให้หรือสามารถนำไปสู่การหยุดชะงัก ความสูญเสีย ภาวะฉุกเฉิน หรือสภาวะวิกฤต
Incident Response (IR)	การดำเนินการเพื่อตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
Impact	ระดับของความเสียหายหรือความสำคัญเมื่อเกิดเหตุการณ์ทางไซเบอร์
Information Security	การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขว้าง เปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหายถูกทำลาย หรือล่วงรู้โดยมิชอบ
Information System	ระบบสารสนเทศที่สนับสนุนการเสริมสร้างขีดความสามารถกองทัพอากาศในส่วนที่เกี่ยวข้องกับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางโดยตรง
Information Security Incident	สถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ อุบัติการณ์ เหตุขัดข้อง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม
Information Security Event	เหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริหารหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนต่อนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

Integrity	การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ ขณะที่มีการใช้งาน ประมวลผล โอน หรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลง แก้ไข ทำให้สูญเสีย ทำให้เสียหาย หรือถูกทำลาย โดยไม่ได้รับอนุญาตหรือโดยมิชอบ
Internal Threats	การคุกคามและการโจมตีจากภายในองค์กร
Intrusion	การบุกรุกที่อาจจะก่อให้เกิดอันตรายต่อระบบหรือข้อมูลต่าง ๆ
Investigation Cyber	การสืบสวนอาชญากรรมไซเบอร์
IP Spoofing	เทคนิคที่ผู้โจมตี/ผู้ไม่ประสงค์ดี นิยมใช้ เพื่อเข้ามายังเครือข่ายภายในองค์กร และทำการโจมตี แบบ DDoS (Distributed Denial-of-Service) ไปยังระบบหรืออุปกรณ์เป้าหมาย ซึ่งส่งผลกระทบต่อความน่าเชื่อถือ ชื่อเสียง และรายได้ขององค์กร
	(L)
Log	การบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ หรือข้อมูลที่มีรายละเอียดแสดงกิจกรรมรูปแบบต่าง ๆ ที่เกิดในระบบคอมพิวเตอร์ หรืออุปกรณ์
	(M)
Main Memory	หน่วยความจำที่มีความเร็วสูงใช้ในการจัดเก็บข้อมูลที่กำลังถูกประมวลผลโดยระบบคอมพิวเตอร์ ส่วนใหญ่จะอยู่ในรูปแบบ Random Access Memory (RAM) เป็นหน่วยความจำที่มีความอ่อนไหวต่อกระแสไฟฟ้า
Malware	ซอฟต์แวร์ที่ไม่ประสงค์ดี (Malicious Software) เป็นซอฟต์แวร์ที่ออกแบบมาเพื่อโจมตีและสร้างความเสียหายให้กับระบบคอมพิวเตอร์
	(N)
Network Attached storage (NAS)	การเชื่อมต่อสื่อสำรองข้อมูลเข้ากับ Local Area Network (LAN)
Network Operation Center (NOC)	ศูนย์ปฏิบัติการเครือข่ายซึ่งประกอบด้วยเจ้าหน้าที่ และเครื่องมือต่าง ๆ ที่ใช้ในการควบคุม ตรวจตรา บริหารงานของเครือข่ายให้สามารถใช้งานได้เป็นปกติ
	(O)
One Time Password (OTP)	การยืนยันตัวตนโดยการใช้รหัสผ่านแค่ครั้งเดียว ในการเข้าสู่ระบบ โดยรหัสผ่านจะถูกกำหนดระยะเวลาการ

	ใช้งาน และหากสิ้นสุดเวลาดังกล่าวจะไม่สามารถนำรหัสมาใช้ได้อีก
Open Web Application Security Project (OWASP)	มาตรฐานความมั่นคงปลอดภัยที่เป็นระบบเปิดของ Web Application ซึ่งจัดทำขึ้นโดยองค์กรไม่แสวงหาผลกำไร เพื่อส่งเสริมความรู้และแนวทางดำเนินการ Web Application Security เพื่อทำให้ระบบมีความมั่นคงปลอดภัย
	(P)
Packet	ชุดข้อมูลหรือหน่วยของข้อมูลในระดับ Network Layer ของ OSI Model
Packet Filtering	การกลั่นกรองแพ็กเกตที่จะเข้าสู่เครือข่าย โดย Firewall
Plain Text	ข้อความปกติ ข้อความที่ต้องการส่งไปยังผู้รับ ซึ่งเป็นข้อมูลที่สามารถอ่านและ เข้าใจได้โดยตรง ไม่ต้องแปล โดยเรียกข้อความแบบนี้ว่า Plain Text หรือ Clear Text
Proxy Server	เครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่เป็นตัวกลางในเชื่อมต่อระหว่างเครือข่ายภายในและภายนอก
Protocol	ข้อกำหนด ระเบียบวิธี เกณฑ์วิธี ที่กำหนดเป็นมาตรฐานสำหรับใช้ในการแลกเปลี่ยนข้อมูลระหว่างเครือข่าย หรือองค์กร เพื่อให้สามารถ สื่อสารข้อมูลได้ โดยเป็นการกำหนดวิธีการส่งข้อมูล การกู้คืนข้อมูลเมื่อเกิดความผิดพลาด และระบุผู้ที่รับข้อมูล
	(S)
Secure Socket Layer (SSL)	เทคนิคการเข้ารหัสช่องทางการสื่อสาร โดยใช้วิธีการเข้ารหัสแบบสมมาตร และอสมมาตรเพื่อทำให้การสื่อสารมีความปลอดภัย ข้อมูลไม่รั่วไหลระหว่างรับส่งผ่านเครือข่าย
Secondary Memory	เป็นหน่วยความจำที่มีหน้าที่ในการเก็บข้อมูลระยะยาว เช่น Hard Disk Drive, Solid State Drive และ Optical Drive เป็นต้น หน่วยความจำประเภทนี้ไม่มีความอ่อนไหวต่อกระแสไฟฟ้า
Security Operation Center (SOC)	ศูนย์เฝ้าระวังการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ ระบบเครือข่าย และระบบรักษาความมั่นคงปลอดภัยสารสนเทศ
Sniffer	โปรแกรมหรืออุปกรณ์ที่ใช้ในการดักจับข้อมูลที่มีการส่งผ่านระบบเครือข่าย

Single Sign-On (SSO)	ความสามารถของระบบการยืนยันตัวบุคคล ที่รองรับการให้ผู้ใช้งานลงชื่อเข้าใช้งานระบบ (Login) ครั้งเดียว แล้วสามารถเข้าใช้งานระบบหลายระบบได้ โดยไม่ต้องลงชื่อเข้าใช้งานซ้ำอีก
Security Information and Support Information System (SIS)	ระบบสารสนเทศเพื่อการสนับสนุนของกองทัพอากาศ
Event Management (SIEM) ระบบ	ระบบวิเคราะห์ ข้อมูลจากบันทึกกิจกรรม (Log) จากสารสนเทศหนึ่งระบบหรือหลาย ๆ ระบบรวมกัน โดยองค์กรเป็นผู้กำหนดเกณฑ์การวิเคราะห์ว่าเหตุการณ์ที่เกิดขึ้นเป็นอันตราย หรือไม่เป็น อันตราย
Storage Area Network (SAN)	เทคโนโลยีที่มีประสิทธิภาพสูง โดยเป็นการเชื่อมต่อของอุปกรณ์จัดเก็บข้อมูลจากหลายแหล่งเข้าด้วยกันและทำงานร่วมกันในเครือข่ายอย่างมีประสิทธิภาพ
Syslog Server	เครื่องคอมพิวเตอร์แม่ข่ายสำหรับการให้บริการจัดเก็บข้อมูลกิจกรรม Syslog คอมพิวเตอร์หรืออุปกรณ์ที่ติดตั้งซอฟต์แวร์สำหรับจัดเก็บข้อมูลกิจกรรมแบบ Syslog
	(T)
Trusted Host	โฮสต์ต้นทางที่เป็นโฮสต์จริงที่ทำงานอยู่ในเครือข่าย
	(V)
Virtual Private Network (VPN)	เครือข่ายเสมือนสำหรับใช้งานส่วนตัวหรือเฉพาะ ภายในหน่วยงาน ซึ่งสร้างอยู่บนเครือข่ายจริง ใช้ในการรับส่งข้อมูลให้มีความมั่นคงปลอดภัยและมีความเป็นส่วนตัว
Volatility	ความอ่อนไหวต่อกระแสไฟฟ้าของข้อมูล ข้อมูลที่มีความอ่อนไหวต่อกระแสไฟฟ้า
Vulnerability	จุดอ่อน ข้อบกพร่องด้านความมั่นคงปลอดภัยสารสนเทศของทรัพย์สินสารสนเทศ ที่พบในระบบสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย ทั้งประเภทซอฟต์แวร์และฮาร์ดแวร์ ซึ่งอาจนำไปสู่การเกิดภัยคุกคาม หรือช่องทาง

เอกสารอ้างอิง

Amazon Web Service. (2565, 11). *การรักษาความปลอดภัยทางไซเบอร์คืออะไร*. Abstract retrieved from https://aws.amazon.com/th/what-is/cybersecurity/

America's Cyber Defense Agency. (2022, 4). *Critical Infrastructure Sectors*. Abstract retrieved from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Drew Robb. (2022, 3). *Top 10 Network Access Control (NAC) Solutions*. Abstract retrieved from https://www.esecurityplanet.com/products/network-access-control-solutions/

NIST. (2018, 4). *NIST Releases Version 1.1 of its Popular Cybersecurity Framework.* Abstract retrieved from https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

NT Cyfence. (2565, 10). *SIEM หัวใจของการตรวจจับภัยคุกคามไซเบอร์*. Abstract retrieved from https://www.cyfence.com/article/what-is-siem/

NT Cyfence. (2560, 12). *ทำความรู้จักกับ NIST Cybersecurity Framework*. Abstract retrieved from https://www.cyfence.com/article/nist-cybersecurity-framework/

Prinya. (2565, 9). *กรอบการดำเนินงานด้านความมั่นคงทางไซเบอร์ระดับโลก*. Abstract retrieved from https://www.prinya.org/2022/02/25/กรอบการดำเนินงานด้านคว/

Pryn. (2556, 10). *องค์ประกอบของความมั่นคงปลอดภัยของสารสนเทศ.* Abstract retrieved from http://www.club27001.com/2013/08/normal-0-false-false-false-en-us-x-none.html

Security Blue Team. (2022, 4). *We Train Technical Cyber Defenders*. Abstract retrieved from https://securityblue.team

Team my Inside. (2563, 12). *รู้จัก Two-Factor Authentication ระบบยืนยันตัวตน 2 ชั้น ป้องกันบัญชีถูกแฮก*. Abstract retrieved from https://www.extremeit.com/two-factor-authentication

Tech Talk Thai. (2564, 12). SIEM คืออะไร? ทำไม SIEM ถึงจำเป็นต่อธุรกิจองค์กร?. Abstract retrieved from https://www.techtalkthai.com/what-is-siem/

Throughwave. (2554, 3). *เลือก Network Access Control (NAC) อย่างไรให้เหมาะสมกับองค์กร?*. Abstract retrieved from https://www.throughwave.co.th/2011/03/09/network-access-control-เลือกอย่างไรให้เหมา/

Wikipedia. (2555, 3). *การควบคุมการเข้าถึงเครือข่าย*. Abstract retrieved from https://hmong.in.th/wiki/Network_access_control

Witskyii. (2553, 8). *นวัตกรรมของระบบรักษาความปลอดภัยสำหรับเครือข่าย (NAC)*. Abstract retrieved from https://www.bloggang.com/m/mainblog.php?id=knowled&month=26-08-2010&group=4&gblog=4