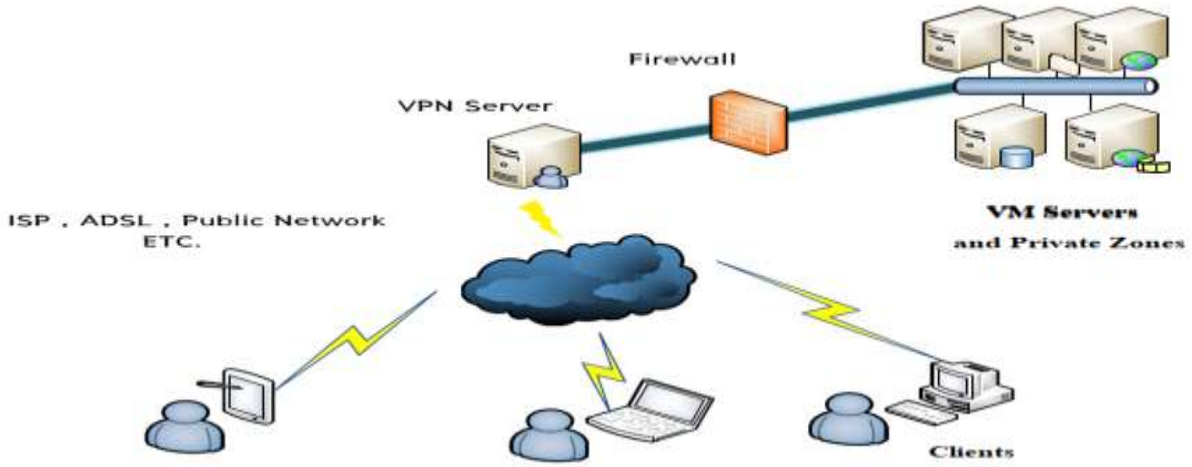
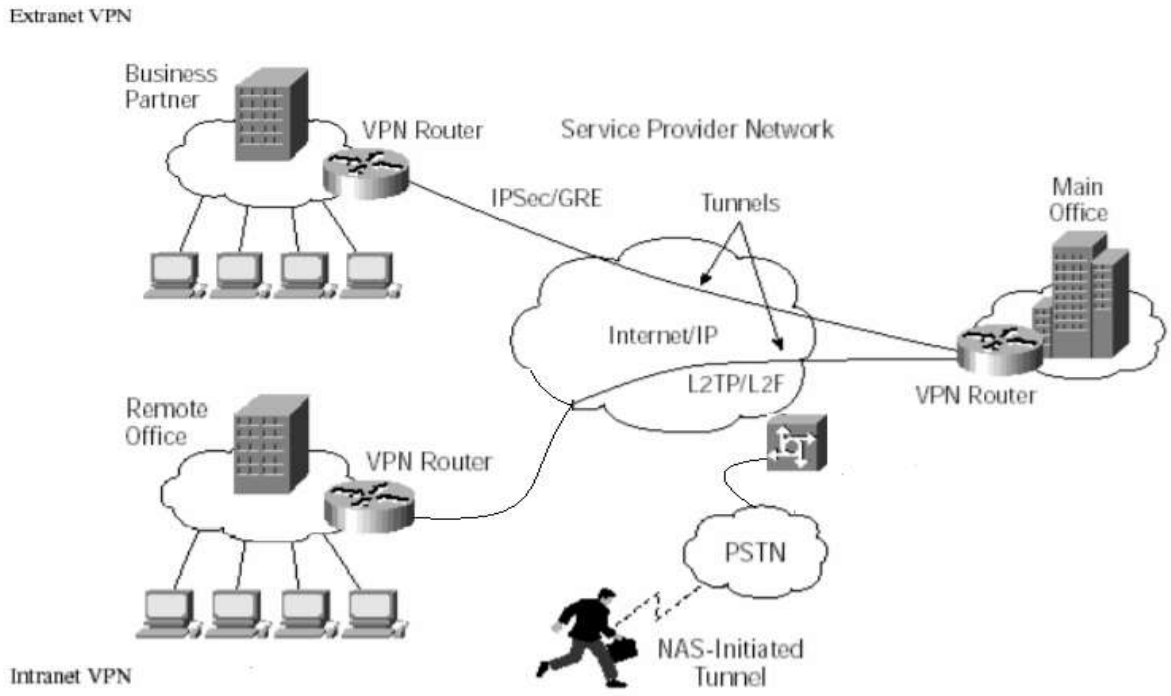
สิ่งที่สำคัญต้องดำเนินการความมั่นคงปลอดภัยสารสนเทศ by TaskS

การดำเนินการความมั่นคงปลอดภัยสารสนเทศ สิ่งสำคัญ ได้แก่ การกำหนดนโยบายการความมั่นคงปลอดภัยสารสนเทศ การจัดการระบบเครือข่าย การจัดการความปลอดภัยของข้อมูล

การจัดการระบบเครือข่าย



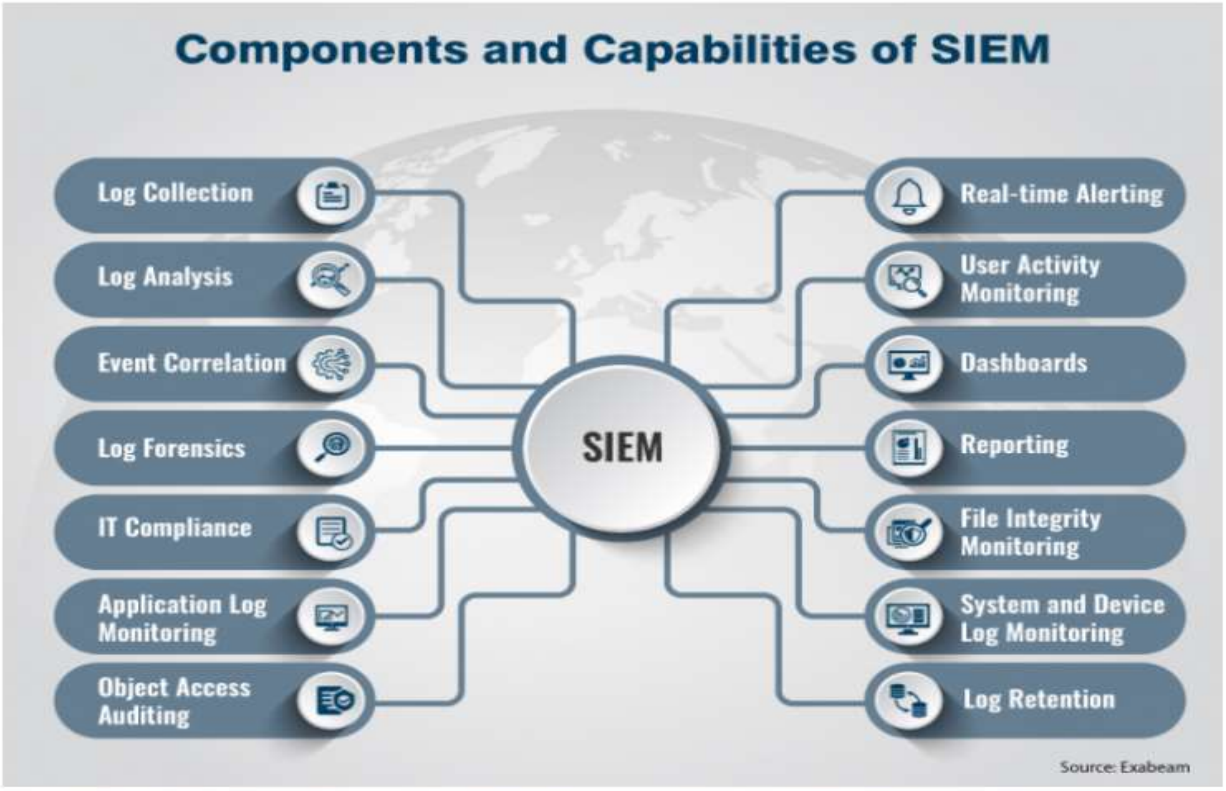
1) การควบคุมระบบการสื่อสาร (Communication control) คือ การป้องกันการเข้าถึงระบบการสื่อสารของเครือข่าย โดยการทำ Virtual Private Network: VPN ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อปกป้องความเป็นส่วนตัวออนไลน์ การปิดกั้นการเข้าถึงเนื้อหาเพื่อเข้าถึงเนื้อหา และควรกำหนดโซน (Zone) เพื่อแยกกลุ่มสะดวกต่อการตรวจสอบและติดตาม



2) การควบคุมระบบไฟร์วอลล์ (Firewall control) คือ ซอฟต์แวร์หรือฮาร์ดแวร์ในระบบเครือข่าย หน้าที่ของไฟร์วอลล์ คือ เป็นตัวกรองข้อมูลสื่อสาร โดยการกำหนดกฎระเบียบมาบังคับใช้ โดยเฉพาะเรื่องของการควบคุมดูแลระบบเครือข่าย ควรกำหนดการแบ่งกลุ่มให้ชัดเจน เพื่อสามารถหาความผิดพลาดของการระบบและตรวจสอบช่องโหว่ได้ง่าย และนำไปสู่สาเหตุของการโจรกรรมข้อมูลทางคอมพิวเตอร์ได้

3) การเปิดใช้งานบริการพอร์ต (Service ports) ที่เชื่อมต่อตามความจำเป็น พร้อมทั้งมีวิธีการเพื่อระบุถึงอุปกรณ์ที่เชื่อมต่อ (Authenticate) อย่างชัดเจน และที่สำคัญควรหลีกเลี่ยงการใช้ หมายเลขพอร์ตที่มีการกำหนดมาให้ เช่น ฐานข้อมูล MariaDB and MySQL มีการกำหนดหมายเลขพอร์ต 3306 ควรเปลี่ยนเป็นหมายเลขพอร์ตที่ไม่ใช้งาน 3808 เป็นต้น

4) การบันทึกแฟ้มร่องรอยของเครือข่าย (Log file network) คือ การจัดเก็บหลักฐาน (Logs) เพื่อติดตามตรวจสอบการทำงานที่เกี่ยวข้องหรืออาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ โดยใช้เทคโนโลยี Security Information and Event Management: SIEM จะช่วยองค์กรในการเก็บรวบรวมข้อมูล Logs จากอุปกรณ์รักษาความปลอดภัยทางไซเบอร์ ซึ่งผู้ที่เกี่ยวข้องในการดูแลระบบไซเบอร์ขององค์กรไม่ว่าจะเป็น System Administrator or Server Administrator (ผู้ดูแลระบบหรือ ผู้ดูแลเซิร์ฟเวอร์) Security Administrator (ผู้ดูแลด้านความปลอดภัย) Security Analyst (นักวิเคราะห์ด้านความปลอดภัย) Auditor (ผู้ตรวจสอบ) Management Team (ผู้บริหารองค์กร)



ภาพจาก https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/components-and-capabilities-of-siem/

การจัดการความปลอดภัยของข้อมูล

ที่มา: https://4.bp.blogspot.com/-OsguVU55F1E/W0X8Y3cpnWI/AAAAAAAABps/DVwYTbmMd64vJL30sRBZP5uKNry-bH3FACLcBGAs/s1600/opentext-graphic-for-web-information-security-en.jpg

1) ความลับ (Confidentiality) คือ การรักษาความลับเป็นการรับประกันว่าผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ ได้แก่ Login/Password และต้องกำหนดให้ยากต่อการเดา

2) ความคงสภาพ (Integrity) คือ ความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลก ประกอบด้วย 2 ส่วน คือ การป้องกัน (Prevention) และการตรวจสอบ (Detection)

2.1) การป้องกัน (Prevention) การเปลี่ยนแปลงแก้ไขข้อมูลโดยผู้ที่ไม่ได้รับอนุญาต รวมถึงป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลนอกเหนือขอบเขตของผู้ได้รับอนุญาต ซึ่งอาจใช้การพิสูจน์ตัวตน (Authentication) และการควบคุมการเข้าถึง (Access Control) ในประเด็นแรก และใช้การตรวจสอบสิทธิ์ (Authorization) ในประเด็นหลัง

2.2) การตรวจสอบ (Detection) เพื่อดูว่าข้อมูลยังคงมีความน่าเชื่อถือหรือไม่ ซึ่งสามารถตรวจเช็ควิเคราะห์เหตุการณ์ต่าง ๆ ที่เกิดขึ้นจาก Log File

3) ความพร้อมใช้ (Availability) คือ ความสามารถในการใช้ข้อมูลหรือทรัพยากรเมื่อต้องการ จัดเป็นส่วนหนึ่งของความมั่นคง ความน่าเชื่อถือ (Reliability) ของระบบ ได้แก่ การจัดทำระบบสำรอง (Backup System)

4) ความปลอดภัยในการป้องกันไวรัส (Antivirus security) คือ ความสามารถในการป้องกันไวรัส เลือกใช้โปรแกรมป้องกันไวรัสที่เหมาะสมหรือตามที่องค์กรกำหนด และทำการอัพเดตให้โปรแกรมป้องกันไวรัสมีฐานข้อมูลของไวรัสล่าสุดจนถึงวันที่ติดตั้งโปรแกรม รวมถึงการอัพเดตระบบ Patch OS