<u>เอกสารชี้แจงผลิตภัณฑ์ SRAN</u>

โดยทางบริษัทโกลบอลเทคโนโลยี อินทิเกรเท ด จำกัด ผู้ริเริ่มพัฒนาผลิตภัณฑ์ด้านระบบป้องกันภัยคุกคามบนเครือข่ายสารสนเทศ ภายใต้แบรนด์ “SRAN” ได้ทำการสำรวจข้อมูลความต้องการและความพึงพอใจของลูกค้า พบว่ามีการสื่อความเข้าใจในผลิตภัณฑ์ที่ไม่ถูกต้องนัก โดยจำกัดความอุปกรณ์ “SRAN” ว่าเป็นอุปกรณ์จัดเก็บ Log เท่านั้น จึงส่งผลกับการนำไปติดตั้งและใช้งานไม่ถูกต้อง ทำให้เกิดปัญหากับการใช้งานของลูกค้าหรือผู้ใช้งาน โดยอุปกรณ์ภายใต้แบรนด์ “SRAN” ไม่ใช่เป็นเพียงอุปกรณ์จัดเก็บ Log เท่านั้น แต่เป็นอุปกรณ์ที่ช่วยใน **“การเฝ้าระวังภัยคุกคามบนเครือข่าย”** ปัญหาที่เกิดจากการเข้าใจผิด ทำให้การนำอุปกรณ์ไปติดตั้ง มีปัญหาระบบล่มหรือรองรับข้อมูลจราจรที่มีการใช้งานภายในเครือข่ายที่นำไปติดตั้งไม่เพียงพอ ส่งผลต่อการเข้าใจผิดของลูกค้า

ในการติดตั้งอุปกรณ์ “SRAN” ไม่ใช่การส่ง Log จากอุปกรณ์ทั้งหมดในเครือข่าย มายังที่อุปกรณ์เพียงเพื่อจัดเก็บข้อมูลจราจร ตามพรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 โดยในเนื้อหาของพรบ. นั้นได้กำหนดประเภทของข้อมูลจราจรในการจัดเก็บเอาไว้ว่ามีประเภทใดบ้าง แต่ปัญหาที่พบก็คือ มีการนำข้อมูลจราจรทั้งหมดที่เกิดขึ้นภายในเครือข่ายส่งมาจัดเก็บที่อุปกรณ์เพียงอุปกรณ์เดียว ซึ่งส่งผลให้อุปกรณ์รองรับข้อมูลจราจรที่มีการใช้งานภายในเครือข่ายไม่เพียงพอ โดยไม่ทำการคัดเลือกเฉพาะข้อมูลที่จำเป็นในการจัดเก็บ ทั้งนี้อุปกรณ์ SRAN มีความสามารถในการเฝ้าระวังภัยคุยคามบนเครือข่าย รวมทั้งสามารถตรวจสอบและจัดเก็บข้อมูลจราจร ตามพรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นผลให้เกิดกรณีที่มีความเข้าใจผิด ในการใช้ความสามารถในการจัดเก็บข้อมูลจราจรผิดวิธีการ ทำให้มีการจัดเก็บข้อมูลจราจรบนเครือข่ายเกิดความซ้ำซ้อนกัน ส่งผลให้เกิดปัญหาที่กล่าวไว้ข้างต้นได้

โดยการจัดเก็บข้อมูลจราจรของอุปกรณ์ SRAN สามารถแบ่งออกเป็น 2 รูปแบบ ดังนี้

1. ใช้ความสามารถในการตรวจสอบและจัดเก็บข้อมูลจราจรบนเครือข่าย โดยใช้การติดตั้งทั้งในแบบขวางอุปกรณ์ (Inline or Transparent Mode) หรือแบบใช้ความสามารถของอุปกรณ์ Switch โดยการ Mirroring Port (Passive Mode) ส่งข้อมูลมาให้

2. ใช้ความสามารถในการรับ Log จากอุปกรณ์อื่นๆ ผ่านการส่ง Syslog Protocol มายังที่อุปกรณ์

ทั้งนี้จากการติดตั้งทั้ง 2 แบบนั้น ทำให้เกิดกรณีที่ว่า มีการติดตั้งและปรับแต่งการทำงานทั้ง 2 แบบขึ้น จึงทำให้มีการจัดเก็บข้อมูลที่ซ้ำซ้อนกัน ยกตัวอย่างเช่น ใช้ความสามารถที่ 1 และยังมีการส่งข้อมูลจราจรในแบบที่ 2 ของอุปกรณ์ Firewall มายังที่อุปกรณ์ ซึ่งส่งผลให้มีการจัดเก็บข้อมูลซ้ำซ้อนมากเป็น 2 เท่า ทำให้มีการใช้พื้นที่ในการจัดเก็บเป็นจำนวนมาก และยังส่งผลให้จัดเก็บข้อมูลที่ไม่จำเป็น ทั้งยังส่งผลให้อุปกรณ์ไม่สามารถรองรับการทำงานได้เพียงพอ

เอกสารชี้แจงผลิตภัณฑ์ต้องการให้ผู้ติดตั้งหรือผู้ใช้งานสามารถนำอุปกรณ์ไปใช้อย่างถูกวิธีและมีประสิทธิภาพมากที่สุด และส่งผลต่อความพึงพอใจของลูกค้าและใช้ประโยชน์จากผลิตภัณฑ์ได้อย่างเต็มประสิทธิภาพ