Black Course

(In-Depth Troubleshooting and Analysis)

Course Overview

สำหรับการอบรมในหลักสูตรนี้ประกอบไปด้วย 2 วัน วันละ 5 ชั่วโมง โดยเนื้อหาเกี่ยวข้องกับการใช้งานเชิงประยุกต์ Black Course จะเป็นหลักสูตรที่เหมาะสำหรับผู้ใช้งาน SRAN ในเชิงประยุกต์และมีความรู้คุณสมบัติ SRAN เบื้องต้นแล้ว ดังนั้นการอบรมในหลักสูตรนี้จึงเน้นไปที่การปฏิบัติงาน เพื่อใช้ในการตรวจหาความผิดปกติเพื่อใช้ในการสืบค้นหาการกระทำความผิดเกี่ยว กับคอมพิวเตอร์ และใช้ในการแก้ไขปัญหาที่อาจจะพบจากการติดตั้งระบบได้อย่างถูกต้อง พร้อมทั้งสามารถเขียนเอกสารวิเคราะห์ความเสี่ยงที่เกิดจากการเฝ้าระวังภัย คุกคามต่าง ๆ จากการใช้งานระบบไอซีทีผ่านอุปกรณ์ SRAN ได้อย่างเหมาะสม

Course Objectives

ผู้เข้าอบรม ต้องเข้าใจในเรื่องต่าง ๆ ดังนี้

- สามารถออกแบบแผนผังระบบเครือข่ายคอมพิวเตอร์ พร้อมตัดสินใจในการติดตั้งอุปกรณ์ SRAN ได้อย่างถูกต้อง ทั้งกรณีที่ต้องติดตั้ง แบบ In-Line, Passive และ Transparent ในแต่ละรูปแบบของระบบเครือข่ายคอมพิวเตอร์
- สามารถแก้ไขสถานะการณ์ฉุกเฉิน โดยการใช้คำสั่ง (Command line) เพื่อควบคุมอุปกรณ์ SRAN ได้อย่างถูกต้อง
- สามารถวิเคราะห์ภัยคุกคามเชิงลึกที่เกิดขึ้นผ่าน Web GUI ของระบบ SRAN ได้อย่างถูกต้อง

Product Used

SRAN Security Center หรือ SRAN Light

Product Trained On

SRAN Security Center หรือ SRAN Light

Prerequisites

- มีความรู้ความเข้าใจด้านภัยคุกคามใหม่ที่เกิดขึ้นจากการใช้งานระบบสารสนเทศ
- เข้าใจถึงหลักการในการนำระบบเฝ้าระวังภัยคุกคามทางอินเตอร์เน็ตและการวิเคราะห์ข้อมูลจาก SRAN บนระบบเครือข่ายคอมพิวเตอร์ขององค์กร

Who Should Attend

สำหรับบุคลากร หรือบุคคลที่มีความเกี่ยวข้องกับการใช้งานอุปกรณ์ SRAN ที่ต้องการวิเคราะห์ในเชิงลึก เพื่อบริหารความปลอดภัยและเฝ้าระวังภัยคุกคาม เครือข่ายสารสนเทศ และเก็บบันทึกข้อมูลจราจรอย่างถูกวิธี

Course Topics

Day 1

เรื่องที่ 1 – Integrated NSM (Network Security Monitoring)

- เรียนรู้ความหมาย NSM การใช้ SRAN เพื่อใช้ในงานเฝ้าระวังภัยคุกคามทางอินเตอร์เน็ตและการใช้งานระบบไอทีภายในองค์กร

เรื่องที่ 2 – Implementation and Configurations

- เรียนรู้การรูปแบบการติดตั้ง SRAN (SRAN Network Topology)
- การใช้ SRAN วิเคราะห์ข้อมูลปกติ (Normal Traffic) เมนูที่ควรใช้พิจารณา
- การใช้ SRAN วิเคราะห์ข้อมูลผิดปกติ (Threat Traffic) เมนูที่ควรใช้พิจารณา
- การออกแบบให้ SRAN ในรุ่น Hybrid สามารถรับค่า syslog ได้อย่างเหมาะสม
- เรียนรู้การควบคุมการใช้งาน SRAN บนเครือข่ายคอมพิวเตอร์ภายในองค์กร และนอกองค์กร ได้แก่ การเข้าถึงระบบ (Authentication System) บนระบบ SRAN, ระดับสิทธิในการเข้าถึงข้อมูลบนระบบ SRAN, การสืบค้นข้อมูลจาก SRAN การประเมินประสิทธิภาพ SRAN ในระบบเครือข่าย, เรียนรู้การทำระบบ Archive Log ที่อุปกรณ์ SRAN ได้เก็บบันทึก

เรื่องที่ 3 – Analysis and Forensic : เพื่อเรียนรู้ถึงลักษณะการโจมตีที่เกิดขึ้นบนระบบเครือข่ายในแต่ละชนิด

- รูปแบบการโจมตีไวรัสคอมพิวเตอร์ (Botnet/Virus/worm attack)
- รูปแบบการโจมตี DDoS/DoS (Botnet/DDoS/DoS Attack)

- รูปแบบการโจมตีผ่านช่องโหว่ (Botnet/Exploit Attack)
- รูปแบบการโจมตีผ่านเว็บแอฟลิเคชั่น (Web Application Attack)

เรื่องที่ 4 – Case Study : นำอุปกรณ์ SRAN ทำการออกแบบระบบเครือข่ายคอมพิวเตอร์ให้มีความเหมาะสมกับการใช้งาน NSM

- เครือข่ายคอมพิวเตอร์แบบ 1 Link อินเตอร์เน็ต ไม่มีระบบป้องกัน มี Core Switch มี Client 30 เครื่อง
- เครือข่ายคอมพิวเตอร์สำหรับ 2 Link อินเตอร์เน็ต ไม่มีระบบป้องกัน มี Core Switch มี Client 50 เครื่อง
- เครือข่ายคอมพิวเตอร์สำหรับ 1 Link อินเตอร์เน็ต มีระบบป้องกัน มี Core Switch มี Client 30 เครื่อง มี Web Server
- เครือข่ายคอมพิวเตอร์สำหรับ 2 Link อินเตอร์เน็ต มีระบบป้องกัน มี Core Switch มี Client 50 เครื่อง มี Web Server และ Mail Server
- เครือข่ายคอมพิวเตอร์ที่มีระบบป้องกัน และมีหลายสาขาออกอินเตอร์เน็ต มี VLAN Client มากกว่า 100 เครื่อง มี Web Server และ Mail Server
- เครือข่ายคอมพิวเตอร์ที่มี DMZ และมี VLAN แยกตามส่วนงานDay 2

ผลลัพธ์ผู้อบรมจัดทำเอกสารประกอบทำการออกแบบการติดตั้ง SRAN พร้อมคำอธิบาย

Day 2

เรื่องที่ 5 – การวิเคราะห์ปัญหา และ สืบค้นหาลักษณะการใช้งานผิดประเภท

- วิเคราะห์หาความผิดปกติที่เกิดจากการใช้ Bandwidth และสาเหตุให้เครือข่ายเกิดความล่าช้าในการรับส่งข้อมูล
- วิเคราะห์ปัญหาไวรัสคอมพิวเตอร์บนระบบเครือข่ายโดยใช้ SRAN
- วิเคราะห์ปัญหาการขโมยข้อมูลบริษัท (Internal Hacking)
- วิเคราะห์ปัญหาการดักรับข้อมูลโดยมิชอบบนระบบเครือข่ายคอมพิวเตอร์ (Sniffer Attack)

ผลลัพธ์ผู้อบรมจัดทำเอกสารประกอบทำการวิเคราะห์ข้อมูลจาก SRAN พร้อมคำอธิบายAgenda

Agenda Day 1

09:00 – 09:30	Registration
09:30 – 10:00	Overview
10:00 – 10:30	Integrated NSM (Network Security Monitoring)
10:30 – 10:45	Coffee Break
10:45 – 12:00	Implementation and Configurations
12:00 – 13:00	Lunch
13:00 – 14:30	Analysis and Forensic
14.30 – 14.45	Coffee Break
14.45 – 15.30	Case Study

Agenda Day 2

09:00 – 09:30	Registration
09:30 – 10:30	การวิเคราะห์ปัญหา และ สืบค้นหาลักษณะการใช้งานผิดประเภท (part 1)
10:30 – 10:45	Coffee Break
10:45 – 12:00	การวิเคราะห์ปัญหา และ สืบค้นหาลักษณะการใช้งานผิดประเภท (part 2)
12:00 – 13:00	Lunch
13:00 – 14:00	การวิเคราะห์ปัญหา และ สืบค้นหาลักษณะการใช้งานผิดประเภท (part 3)
14.30 – 14.45	Coffee Break
14:45 – 15:30	การวิเคราะห์ปัญหา และ สืบค้นหาลักษณะการใช้งานผิดประเภท (part 4)