เหตุการณ์ที่เลือก: CrowdStrike BSOD

วิเคราะห์เหตุการณ์ CrowdStrike BSOD

สาเหตุเกิดจากการอัปเดตซอฟต์แวร์ Falcon Sensor มีข้อผิดพลาด ทำให้เกิดปัญหา Blue Screen of Death (BSOD) ในระบบปฏิบัติการ Windows ทั่วโลก สาเหตุหลักมาจากข้อผิดพลาดในการพัฒนาซอฟต์แวร์และการทดสอบที่ไม่เพียงพอ

มาตรการความปลอดภัยที่เลือก(Security controls chosen)

1. **การจัดการแพตช์ (Patch Management)**

   - การจัดการแพตช์อย่างมีประสิทธิภาพช่วยให้องค์กรสามารถทดสอบและอัปเดตในสภาพแวดล้อมจำลอง (Sandbox) ก่อนใช้งานจริง เพื่อลดความเสี่ยงการปล่อยเวอร์ชั่นอัปเดตที่มีปัญหา เช่น BSOD ที่เกิดจาก Falcon Sensor
   - มีกระบวนการย้อนกลับ (Rollback) ช่วยให้สามารถกู้คืนระบบได้อย่างรวดเร็วหากเกิดข้อผิดพลาด

2. **การเฝ้าระวัง การบันทึก และการแจ้งเตือน (Monitoring, Logging, and Alerting)**

   - การเฝ้าระวังระบบอย่างต่อเนื่อง ช่วยให้สามารถตรวจจับความผิดปกติ
   - การบันทึกข้อมูลเหตุการณ์ ช่วยเก็บหลักฐานสำคัญสำหรับการวิเคราะห์ต้นเหตุ
   - การแจ้งเตือนแบบเรียลไทม์ ช่วยให้สามารถรู้ปัญหาได้ทันทีและดำเนินการแก้ไขได้อย่างรวดเร็ว เพื่อลดเวลาที่ระบบหยุดการทำงาน

3. **แผนการตอบสนองต่อเหตุการณ์ (Security Incident Response Plan)**

   - มีแผนตอบสนองต่อเหตุการณ์ฉุกเฉินช่วยให้องค์กรสามารถรับมือกับสถานการณ์ได้อย่างมีประสิทธิภาพ
   - ในกรณี BSOD แผนนี้ช่วยให้ทีมงานแยกอุปกรณ์ที่ได้รับผลกระทบ แจ้งแนวทางแก้ไขให้กับผู้ใช้งาน และฟื้นฟูระบบได้อย่างรวดเร็ว เพื่อลดเวลาที่ระบบหยุดการทำงานและผลกระทบต่อธุรกิจ