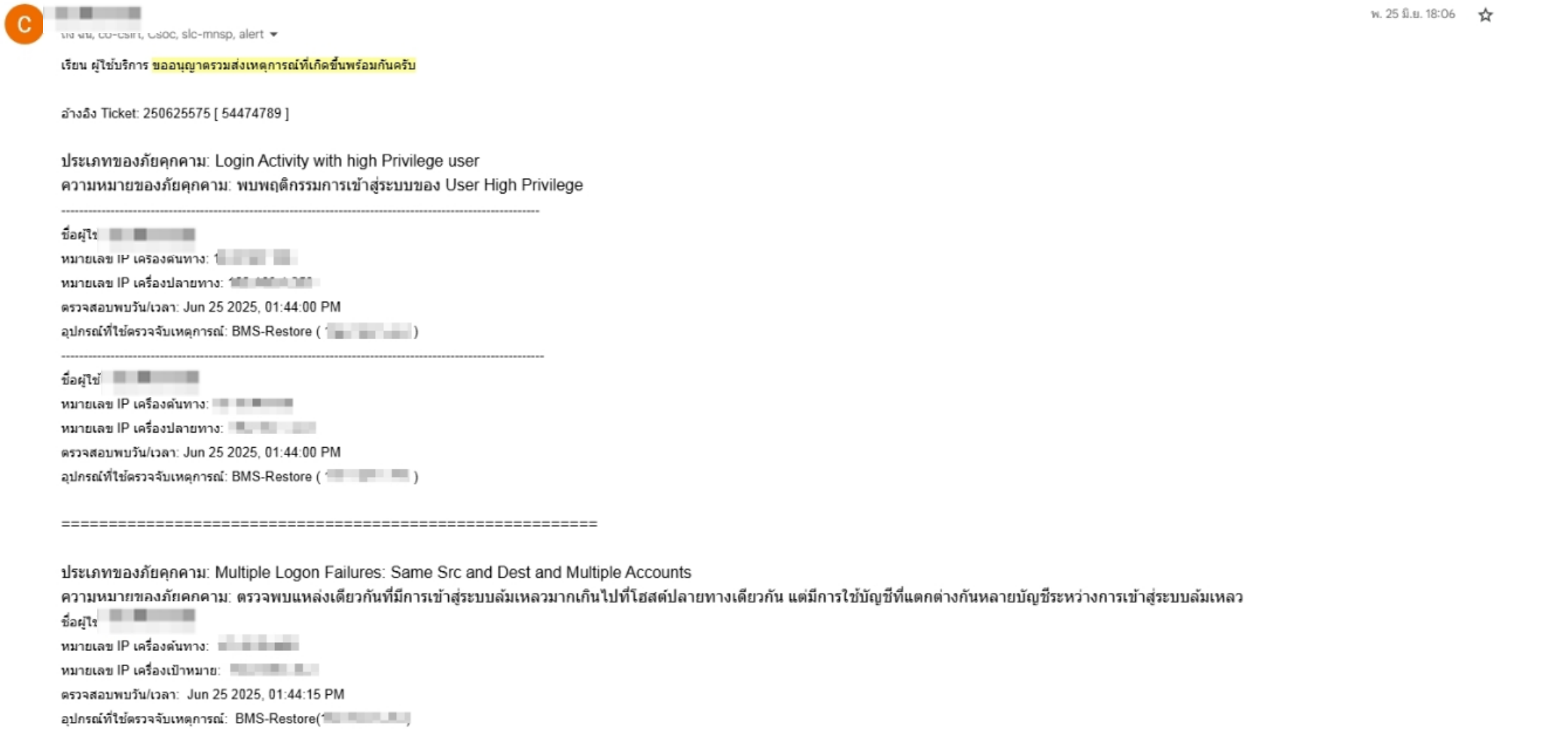
รายงานสถานะการตรวจสอบ Port Whitelist



C [redacted]

[redacted], cc-csirt, csoc, slc-mnsp, alert

พ. 25 มิ.ย. 18:06

เรียน ผู้ใช้บริการ ขออนุญาตรวมส่งเหตุการณ์ที่เกิดขึ้นพร้อมกันครับ

อ้างอิง Ticket: 250625575 [54474789]

ประเภทของภัยคุกคาม: Login Activity with high Privilege user
ความหมายของภัยคุกคาม: พบพฤติกรรมการเข้าสู่ระบบของ User High Privilege

---

ชื่อผู้ใช้ [redacted]
หมายเลข IP เครื่องต้นทาง: [redacted]
หมายเลข IP เครื่องปลายทาง: [redacted]
ตรวจสอบพบวัน/เวลา: Jun 25 2025, 01:44:00 PM
อุปกรณ์ที่ใช้ตรวจจับเหตุการณ์: BMS-Restore ([redacted])

ชื่อผู้ใช้ [redacted]
หมายเลข IP เครื่องต้นทาง: [redacted]
หมายเลข IP เครื่องปลายทาง: [redacted]
ตรวจสอบพบวัน/เวลา: Jun 25 2025, 01:44:00 PM
อุปกรณ์ที่ใช้ตรวจจับเหตุการณ์: BMS-Restore ([redacted])

==========

ประเภทของภัยคุกคาม: Multiple Logon Failures: Same Src and Dest and Multiple Accounts
ความหมายของภัยคุกคาม: ตรวจพบแหล่งเดียวกันที่มีการเข้าสู่ระบบล้มเหลวมากเกินไปที่โฮสต์ปลายทางเดียวกัน แต่มีการใช้บัญชีที่แตกต่างกันหลายบัญชีระหว่างการเข้าสู่ระบบล้มเหลว
ชื่อผู้ใช้ [redacted]
หมายเลข IP เครื่องต้นทาง: [redacted]
หมายเลข IP เครื่องเป้าหมาย: [redacted]
ตรวจสอบพบวัน/เวลา: Jun 25 2025, 01:44:15 PM
อุปกรณ์ที่ใช้ตรวจจับเหตุการณ์: BMS-Restore([redacted])

รายงานสถานะการตรวจสอบ Port Whitelist

C [redacted]

ถึง ฉัน

เรียน ผู้ใช้บริการ

ฝ่ายปฏิบัติการ บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) ขอจัดส่งรายงานตรวจสอบสถานะการ PORT ผ่าน Public IP เพื่อลดความเสี่ยง โดยมีรายละเอียด ดังนี้

ตรวจสอบเมื่อวันที่ : 29/07/2025 09:47:11

เลขที่อ้างอิง : 11019

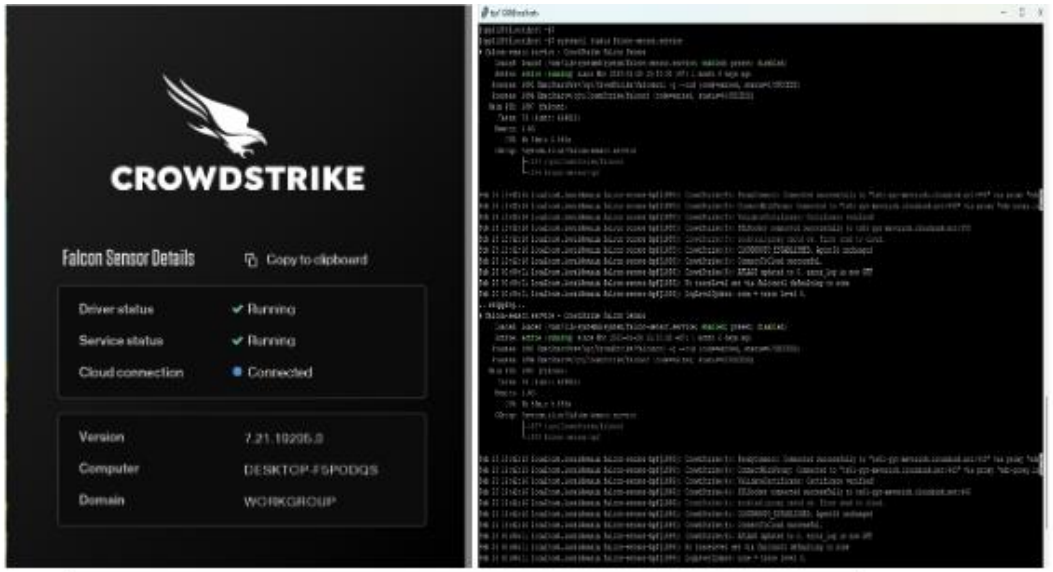
จังหวัด : จ.อุดรธานี

โรงพยาบาล : โรงพยาบาลทุ่งฝน

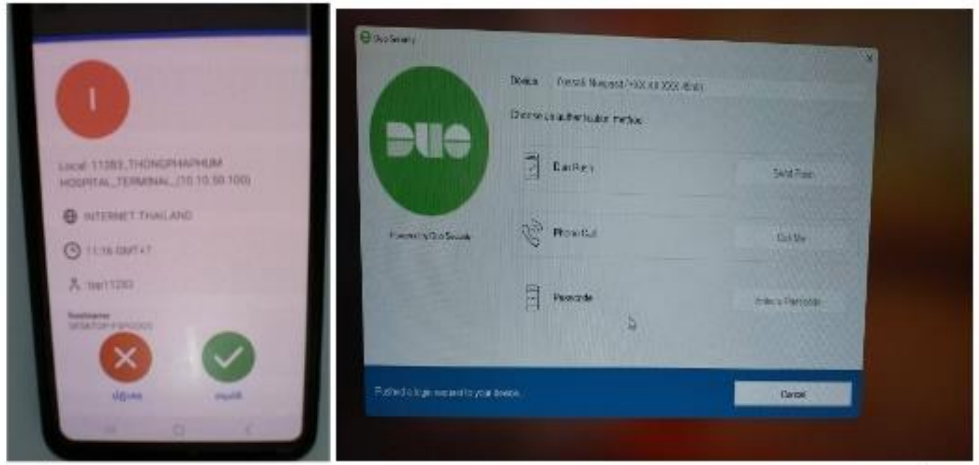
สถานะการตรวจสอบ : ปกติ

No.	VM Name	IP Public	Port (ได้รับการยืนยันจากโรงพยาบาลแล้ว)	ผลการ SCAN PORT ปัจจุบัน
1	-	203.		
2	-	203.		
3	-	203.		
4	-	203.		
5	-	203.		
6	-	203.		

บริหารจัดการและรักษาความปลอดภัยระบบสารสนเทศ (IT Infrastructure & Security)



EDR ติดตั้ง ยี่ห้อ edr crownstrike ติดตั้งให้แก่ Server VM ทุกตัว และเครื่อง terminal หลัก



ระบบ Response ในการยืนยันการเข้าถึงระบบ DUO