สรุปผลการพิจารณาข้อคิดเห็นของผู้ประกอบการ ที่กองทุนฯเผยแพร่ร่างประกาศและร่างเอกสารประกวดราคา
ซื้อระบบป้องกันภัยคุกคามทางเครือข่ายไซเบอร์สำหรับเครื่องคอมพิวเตอร์ปลายทาง (End Point)
ระยะเวลา ๓ ปี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

ลำดับ	วันที่วิจารณ์	ข้อวิจารณ์บริษัท		เนื้อหาวิจารณ์	ผลการพิจารณาของกองทุนฯ
๑	๑๘-ธ.ค.-๖๖	๑	TOR ข้อ ๓.๓ หน้า ๓ ข้อ ๓.๓.๗	๓.๓.๗ สามารถแสดงรายงาน Attack Forensics ในรูปแบบ STIX, IOC, PCAP และ CSV format ได้ **เปลี่ยนแปลงเป็น** สามารถแสดงรายงาน Attack Forensics(IOC) ในรูปแบบ STIX, CSV หรือ PCAP format หรือสามารถใช้งานร่วมกับ STIX/TAXII ได้เป็นอย่างน้อย **เหตุผล** อุปกรณ์รุ่นใหม่ๆ ผลิตภัณฑ์ ต่างๆ มีความสามารถ รองรับ format ไฟล์ที่แตกต่างกัน และมี STIX/TAXII ที่เป็น Trusted Automated eXchange of Inteligent Information มาตรฐานที่เป็นสากล	ยืนยันตามข้อกำหนด เนื่องจากมีความต้องการ การแสดงรายงาน Attack Forensics ที่สามารถแสดงในรูปแบบ STIX, IOC, PCAP และ CSV format ได้เป็นอย่างน้อยโดยสามารถเสนอเพิ่มเติมจากความสามารถเดิมได้ แต่ไม่สามารถปรับให้เป็นข้อเสนออื่นและตัดความสามารถ STIX, IOC, PCAP และ CSV format ได้
		๒	TOR ข้อ ๓.๓ หน้า ๓ ข้อ ๓.๓.๘	๓.๓.๘ สามารถตรวจจับการโจมตีในเครือข่าย เช่น ARP flood, ARP Scan, MITM (Man in the Middle) บน NBNS, mDNS และ SMB Attack ได้ **เปลี่ยนแปลงเป็น** สามารถตรวจจับการโจมตีในเครือข่าย เช่น ARP flood, ARP Scan, MITM (Man in the Middle) บน Network Layer ๒ และ SMB Attack ได้เป็นอย่างน้อย **เหตุผล** Network Layer ๒ จะเป็นการระบุครอบคลุมกว่า NBNS, mDNS ทำให้เกิดประโยชน์สูงสุด	ยืนยันตามข้อกำหนด เนื่องจากในเครือข่ายใน Network Layer ๒ มีหลากหลาย Protocol แต่การโจมตีที่อยู่ในรูปแบบ MITM (Man in the Middle) ที่สำคัญจะมาจากเครื่องคอมพิวเตอร์ของผู้ใช้งานที่เป็น Windows โดยต้องสามารถตรวจจับจาก Protocol NBNS และ mDNS ดังนั้นจึงจำเป็นต้องระบุชื่อ Protocol
		๓	TOR ข้อ ๓.๓ หน้า ๓ ข้อ ๓.๓.๑๘	๓.๓.๑๘ สามารถสร้างกับดักในรูปแบบ Services เช่น FTP/SFTP, HTTP/HTTPS, SMB, SSH, SMTP, SNMP, Telnet, RDP และ Application เช่น MySQL, Apache, Tomcat, Jboss, Subversion, Active Directory ได้ **เปลี่ยนแปลงเป็น** สามารถสร้างกับดักในรูปแบบ Services เช่น FTP/SFTP, HTTP/HTTPS, SMB, SSH, SMTP, SNMP, Telnet, RDP หรือ Application เช่น MySQL, Apache, Tomcat, Jboss, Subversion, Active Directory ได้ **เหตุผล** Application ปกติจะ Based On Service/Protocol อยู่แล้ว ดังนั้นสามารถยึดตาม Service แทนได้ ปรับแก้ไขเพื่อให้ผลิตภัณฑ์อื่นสามารถเข้าแข่งขันได้	ยืนยันตามข้อกำหนด เนื่องจากการสร้างกับดักจำเป็นต้องใช้การสร้างจากทั้ง ๒ ส่วน Service เช่น FTP/SFTP, HTTP/HTTPS, SMB, SSH, SMTP, SNMP, Telnet, RDP และ Application เช่น MySQL, Apache, Tomcat, Jboss, Subversion, Active Directory ได้ เป็นอย่างน้อย ไม่สามารถกำหนดทำงานให้เป็นอย่างใดอย่างหนึ่งได้ เพราะจะทำให้ไม่เกิดประสิทธิภาพ ในการสร้างกับดัก โดยผลิตภัณฑ์อื่นที่สามารถเข้าแข่งขันได้ เช่น SentinelOne, TrapXSecurity, Fidelissecurity เป็นต้น

ลำดับ	วันที่วิจารณ์	ข้อวิจารณ์บริษัท		เนื้อหาวิจารณ์	ผลการพิจารณาของกองทุนฯ
		๔	TOR ข้อ ๓.๓ หน้า ๔ ข้อ ๓.๓.๒๕	๓.๓.๒๕ สามารถแสดงผลข้อมูลผู้ใช้ที่ทำการสืบค้นข้อมูล Active Directory จากเครื่องผู้ใช้งานได้ **เปลี่ยนแปลงเป็น** สามารถแสดงผลข้อมูลผู้ใช้ที่ทำการสืบค้นข้อมูล AD จากเครื่องผู้ใช้งาน หรือแสดงเหตุการณ์จากชื่อผู้ใช้ที่เป็นเหยื่อล่อ โดยนำเข้ามาจาก AD ได้ **เหตุผล** ปรับแก้ไขเพื่อให้ผลิตภัณฑ์อื่นสามารถเข้าแข่งขันได้	ยืนยันตามข้อกำหนด เนื่องจากการสืบค้นข้อมูลผู้ใช้จาก Active Directory ได้โดยตรงจะสามารถป้องกันการโจมตี Active Directory ได้มีประสิทธิภาพมากกว่าการสืบค้นข้อมูลเฉพาะชื่อผู้ใช้ที่เป็นเหยื่อล่อ โดยนำเข้ามาจาก Active Directory โดยมีผลิตภัณฑ์อื่นที่สามารถเข้าแข่งขันได้ เช่น SentinelOne, TrapXSecurity,Fidelissecurity เป็นต้น
		๕	TOR ข้อ ๓.๓ หน้า ๔ ข้อ ๓.๓.๒๖	๓.๓.๒๖ สามารถทำ Whitelist หรือ Blacklist กรณี Process, User, Endpoint ที่จะใช้สืบค้นข้อมูล Active Directory ตัวจริงได้ **เปลี่ยนแปลงเป็น** สามารถทำ Whitelist หรือ Blacklist กรณี Process, User, Endpoint ที่จะใช้สืบค้นข้อมูล Active Directory ตัวจริง หรือ Quarantine Endpoint ที่พยายามเข้าถึงบริการที่เป็นเหยื่อล่อบนเครื่อง Active Directory ได้ **เหตุผล** ปรับแก้ไขเพื่อให้ผลิตภัณฑ์อื่นสามารถเข้าแข่งขันได้	ยืนยันตามข้อกำหนด เนื่องจากการป้องกันการสืบค้นข้อมูล Active Directory ตัวจริงเป็นการป้องกันการโจมตี Active Directory ได้โดยตรงแต่การ Quarantine Endpoint ที่พยายามเข้าถึงบริการที่เป็นเหยื่อล่อบนเครื่อง Active Directory จะไม่สามารถป้องกันได้ ซึ่งจะเป็นเพียงการตรวจจับผู้ที่พยายามโจมตีเหยื่อล่อเท่านั้น โดยมีผลิตภัณฑ์อื่นที่สามารถเข้าแข่งขันได้ เช่น SentinelOne, TrapXSecurity, Fidelissecurity เป็นต้น