ข้อกำหนดรายละเอียดคุณลักษณะเฉพาะ (Term of Reference: TOR)
รายการ ระบบรักษาความปลอดภัยเว็บไซต์สำหรับการเรียนรู้ออนไลน์ จำนวน 1 ระบบ
สำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

1. ความเป็นมาและวัตถุประสงค์

ระบบรักษาความปลอดภัยเว็บไซต์ (Web Application Firewall) เป็นระบบหลักที่มีหน้าที่ในการปกป้องเว็บไซต์และเว็บแอปพลิเคชันจากภัยคุกคามและการโจมตีที่มุ่งร้าย โดยทำงานระหว่างผู้ใช้งานและเว็บแอปพลิเคชันเพื่อกรองและป้องกันการเข้าถึงที่เป็นอันตราย ซึ่งปัจจุบันระบบดูแลรักษาความปลอดภัยเว็บไซต์ที่ให้บริการอยู่ภายในมหาวิทยาลัย จำนวน 221 เว็บไซต์ อาทิเช่น ระบบเรียนการสอนออนไลน์ (mooc) ระบบสารสนเทศนักศึกษา (REG) เว็บไซต์ของคณะต่าง ๆ ภายในมหาวิทยาลัย ระบบสารสนเทศทรัพยากรมนุษย์ (HRIS) ระบบจัดการบัญชีผู้ใช้งาน ICIT Account และระบบวารสารมหาวิทยาลัยเป็นต้น รวมถึงรักษาความปลอดภัยของเครื่องแม่ข่ายเสมือนจำนวน 130 เครื่อง ที่ให้บริการแก่หน่วยงานต่าง ๆ ภายในมหาวิทยาลัย จากปริมาณการใช้งานระบบเว็บแอปพลิเคชันและจำนวนเว็บไซต์ที่เพิ่มขึ้นภายในมหาวิทยาลัยส่งผลให้มหาวิทยาลัยต้องเผชิญกับความเสี่ยงจากการโจมตีทางไซเบอร์มากขึ้น ข้อมูลสำคัญของมหาวิทยาลัยเสี่ยงต่อการ ถูกขโมย ถูกทำลาย หรือถูกนำไปใช้ในทางที่ไม่เหมาะสม อาจส่งผลต่อชื่อเสียง และความน่าเชื่อถือต่อมหาวิทยาลัยได้ในระยะยาว สำนักคอมพิวเตอร์ฯ เล็งเห็นถึงความสำคัญต่อความเสี่ยงดังกล่าว จึงมีความประสงค์จัดหาระบบรักษาความปลอดภัยเว็บแอปพลิเคชัน (Web Application Firewall) ที่สามารถป้องกันและกรองการโจมตีทาง ไซเบอร์ได้อย่างมีประสิทธิภาพ เพื่อรักษามาตรฐานการให้บริการข้อมูลให้มีความปลอดภัยและน่าเชื่อถือ ตลอดจนสร้างความมั่นใจให้กับผู้ใช้บริการทุกกลุ่ม

2. คุณสมบัติของผู้ยื่นข้อเสนอ

2.1 มีความสามารถตามกฎหมาย

2.2 ไม่เป็นบุคคลล้มละลาย

2.3 ไม่อยู่ระหว่างเลิกกิจการ

2.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

2.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

2.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

2.7 เป็นนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว

2.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอราคารายอื่นที่เข้ายื่นข้อเสนอให้แก่ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันราคาอย่างเป็นธรรม ในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้

2.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทยเว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งสละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

1.....ประธาน 2.....กรรมการ 3.....กรรมการและเลขานุการ

2.10 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ "กิจการร่วมค้า" ต้องมีคุณสมบัติดังนี้

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักข้อตกลงระหว่างผู้เข้าร่วมค้าจะต้องมีการกำหนดสัดส่วนหน้าที่และความรับผิดชอบในปริมาณงานสิ่งของหรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก กิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลัก ผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

กรณีที่ข้อตกลงระหว่างผู้เข้าร่วมค้ากำหนดให้มีการมอบหมายผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า การยื่นข้อเสนอดังกล่าวไม่ต้องมีหนังสือมอบอำนาจ

สำหรับข้อตกลงระหว่างผู้เข้าร่วมค้าที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้ยื่นข้อเสนอผู้เข้าร่วมค้าทุกรายจะต้องลงลายมือชื่อในหนังสือมอบอำนาจให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้ยื่นข้อเสนอในนามกิจการร่วมค้า

2.11 ผู้ยื่นข้อเสนอต้องลงทะเบียนที่มีข้อมูลถูกต้องครบถ้วนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement : e-GP) ของกรมบัญชีกลาง

2.12 ผู้ยื่นข้อเสนอต้องมีมูลค่าสุทธิของกิจการ ดังนี้

(1) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยซึ่งได้จดทะเบียนเกินกว่า 1 ปี ต้องมีมูลค่าสุทธิของกิจการ จากผลต่างระหว่างสินทรัพย์สุทธิหักด้วยหนี้สินสุทธิ ที่ปรากฏในงบแสดงฐานะการเงินที่มีการตรวจรับรองแล้ว ซึ่งจะต้องแสดงค่าเป็นบวก 1 ปีสุดท้ายก่อนวันยื่นข้อเสนอ

(2) กรณีผู้ยื่นข้อเสนอเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทย ซึ่งยังไม่มีการรายงานงบแสดงฐานะการเงินกับกรมพัฒนาธุรกิจการค้า ให้พิจารณาการกำหนดมูลค่าของทุนจดทะเบียน โดยผู้ยื่นข้อเสนอจะต้องมีทุนจดทะเบียนที่เรียกชำระมูลค่าหุ้นแล้ว ณ วันที่ยื่นข้อเสนอ ไม่ต่ำกว่า 1 ล้านบาท

(3) สำหรับการจัดซื้อจัดจ้างครั้งหนึ่งที่มีวงเงินเกิน 500,000.00 บาทขึ้นไป กรณีผู้ยื่นข้อเสนอเป็นบุคคลธรรมดา โดยพิจารณาจากหนังสือรับรองบัญชีเงินฝากไม่เกิน 90 วัน ก่อนวันยื่นข้อเสนอ โดยต้องมีเงินฝากคงเหลือในบัญชีธนาคารเป็นมูลค่า 1 ใน 4 ของมูลค่างบประมาณของโครงการหรือรายการที่ยื่นข้อเสนอ ในแต่ละครั้ง และหากเป็นผู้ชนะการจัดซื้อจัดจ้างหรือเป็นผู้ได้รับการคัดเลือกจะต้องแสดงหนังสือรับรองบัญชีเงินฝากที่มีมูลค่าดังกล่าวอีกครั้งหนึ่งในวันลงนามในสัญญา

(4) กรณีที่ผู้ยื่นข้อเสนอไม่มีมูลค่าสุทธิของกิจการหรือทุนจดทะเบียน หรือมีแต่ไม่เพียงพอที่จะเข้ายื่นข้อเสนอ ผู้ยื่นข้อเสนอสามารถขอวงเงินสินเชื่อ โดยต้องมีวงเงินสินเชื่อ 1 ใน 4 ของมูลค่า งบประมาณที่ยื่นข้อเสนอในครั้งนั้น (สินเชื่อที่ธนาคารภายในประเทศ หรือบริษัทเงินทุนหรือบริษัทเงินทุน หลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์ และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยพิจารณาจากยอดเงินรวมของวงเงินสินเชื่อที่สำนักงานใหญ่รับรอง หรือที่สำนักงานสาขารับรอง (กรณีได้รับมอบอำนาจจากสำนักงานใหญ่) ซึ่งออกให้แก่ผู้ยื่นข้อเสนอนับถึงวันยื่นข้อเสนอไม่เกิน 90 วัน)

(5) กรณีตาม (1) - (4) ยกเว้นสำหรับกรณีดังต่อไปนี้

(5.1) กรณีที่ผู้ยื่นข้อเสนอเป็นหน่วยงานของรัฐ

(5.2) นิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยที่อยู่ระหว่างการฟื้นฟูกิจการตามพระราชบัญญัติล้มละลาย (ฉบับที่ 10) พ.ศ. 2561

1.....ประธาน 2.....กรรมการ 3.....กรรมการและเลขานุการ

3. **รายละเอียดคุณลักษณะเฉพาะ** (Term of Reference: TOR)

รายการ ระบบรักษาความปลอดภัยเว็บไซต์สำหรับการเรียนรู้ออนไลน์ จำนวน 1 ระบบ มีรายละเอียดตามเอกสารแนบ

4. **ระยะเวลาส่งมอบพัสดุ**

ภายใน 120 วันนับถัดจากวันลงนามในสัญญา

5. **หลักเกณฑ์ในการพิจารณาคัดเลือกข้อเสนอ**

ในการพิจารณาผลการยื่นข้อเสนอครั้งนี้ มหาวิทยาลัยจะพิจารณาตัดสินโดยใช้เกณฑ์ราคา

6. **วงเงินงบประมาณ/วงเงินที่ได้รับการจัดสรร**

วงเงิน 3,940,000.00 บาท (สามล้านเก้าแสนสี่หมื่นบาทถ้วน)

7. **งวดงานและการจ่ายเงิน**

การจ่ายเงินเป็นไปตามเงื่อนไขที่มหาวิทยาลัยกำหนด

8. **อัตราค่าปรับ**

อัตราร้อยละ 0.20 ของราคาสิ่งของที่ยังไม่ได้รับมอบ

9. **การกำหนดระยะเวลารับประกันความชำรุดบกพร่อง (ถ้ามี)**

ระยะเวลารับประกันความชำรุดบกพร่องไม่น้อยกว่า 1 ปี

1.....ประธาน 2.....กรรมการ 3.....กรรมการและเลขานุการ

ข้อกำหนดรายละเอียดคุณลักษณะเฉพาะ (Term of Reference: TOR)
รายการ ระบบรักษาความปลอดภัยเว็บไซต์สำหรับการเรียนรู้ออนไลน์ จำนวน 1 ระบบ
สำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

1. รายการและจำนวนที่ต้องการ

ระบบรักษาความปลอดภัยเว็บไซต์สำหรับการเรียนรู้ออนไลน์ จำนวน 1 ระบบ ประกอบด้วย

1.1 ระบบรักษาความปลอดภัยเว็บไซต์ (Web Application Firewall) จำนวน 1 ระบบ

1.2 ซอฟท์แวร์ป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (Endpoint Detection and Response) จำนวนไม่น้อยกว่า 10 ลิขสิทธิ์

2. ข้อกำหนดคุณสมบัติของระบบรักษาความปลอดภัยเว็บไซต์ (Web Application Firewall) จำนวน 1 ระบบ ต้องมีคุณสมบัติขั้นต่ำหรืออย่างน้อย ดังต่อไปนี้

2.1 อุปกรณ์ที่นำเสนอจะต้องเป็น Hardware Appliance ทำหน้าที่ในการป้องกันระบบงานด้าน Web Application โดยเฉพาะ

2.2 มี Throughput HTTP ได้ไม่น้อยกว่า 1 Gbps และ Server ได้ไม่น้อยกว่า 150 Server

2.3 มีจำนวน HTTP (Transactions per Second) ไม่น้อยกว่า 90,000 TPS และ HTTP (Connection per Second) ไม่น้อยกว่า 16,000 TPS

2.4 มี Network Interface แบบ 10/100/1000 UTP ไม่น้อยกว่า 8 พอร์ต และทำ bypass ได้

2.5 มี Management Interface จำนวน 1 พอร์ต สำหรับบริหารจัดการอุปกรณ์โดยเฉพาะ

2.6 ต้องบริหารจัดการอุปกรณ์ผ่านโปรแกรม Web Browser และ CLI ได้เป็นอย่างน้อย

2.7 ทำงานแบบ In-line Bridge Mode และ Reverse Proxy Mode รูปแบบ One-Arm Proxy และ Two-Arm Proxy ได้

2.8 ทำงานและปกป้อง Web Application ต่างๆได้โดยรองรับ HTTPS และ HTTP ได้เป็นอย่างน้อย

2.9 ทำงาน Let's Encrypt ในการทำงานแบบ In-line Bridge Mode

2.10 ป้องกันการโจมตีผ่านทาง Web Application และ API Protection ได้ในรูปแบบอย่างน้อยดังนี้

2.10.1 Protection against OWASP

2.10.2 Advanced Bot Protection

2.10.3 API Protection

2.10.4 Server Cloaking

2.10.5 Geo-IP and IP Reputation Checking

2.10.6 Application DDoS Protection

2.10.7 Volumetric DDoS Protection

2.10.8 JSON Security

2.10.9 XML Firewall

2.10.10 Client-Side Protection

2.11 มีเทคโนโลยี Adaptive Profiling ที่เรียนรู้การใช้งานเว็บแอพพลิเคชั่นในรูปแบบ Request Traffic และ Response Traffic จาก Web server โดย Learning Mode และทำเป็น Profile Policy ในการตรวจสอบได้

1.....ประธาน 2.....กรรมการ 3.....กรรมการและเลขานุการ

2.12 มีฟังก์ชั่นการทำงาน Web Application Load Balancing โดยทำ Algorithm เช่น Round-Robin, Weighted Round Robin และ Least Request ได้เป็นอย่างน้อย

2.13 เพิ่มความเร็ว Traffic เพื่อเข้าถึงระบบ Web Application โดยใช้การทำ Caching, Compression หรือ Traffic Optimization เพื่อเพิ่มประสิทธิภาพได้

2.14 มีฟังก์ชั่นการเร่งความเร็วในการเข้าใช้งาน Web server (Web Acceleration)

2.15 ทำงานแบบ SSL Offloading

2.16 ทำการ Add Web Server โดยใช้ IP address และ Port และแยกบริหารจัดการ Domain Name ได้

2.17 ทำงานในลักษณะสำรองระบบ (High Availability) แบบ Active/Active, Active/Standby

2.18 ทำการตรวจสอบ Traffic ได้แบบ Real-time และนำการปรับปรุง Configuration (Auto Configuration Engine) เพื่อเพิ่มประสิทธิภาพในการป้องกันระบบ Web Application ได้

2.19 ป้องกันการโจมตีในรูปแบบ HTTP-base DOS attack เช่น HTTP Flood, Slowloris, RUDY, Slowread เป็นต้น

2.20 มีแหล่งจ่ายไฟ (Power Supply) แบบ Redundant

2.21 มีขนาด 2U และติดตั้งในตู้เก็บอุปกรณ์มาตรฐานขนาด 19 นิ้วได้

2.22 ต้องอัพเดทฐานข้อมูลได้ไม่น้อยกว่า 1 ปี

2.23 เพื่อป้องกันสินค้าลอกเลียนแบบ หรือสินค้าเก่านำมาใช้งานใหม่ ผู้เสนอราคาต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่าย จากบริษัทผู้ผลิต หรือสาขาของผู้ผลิต หรือตัวแทนจำหน่ายในประเทศ

3. ข้อกำหนดคุณสมบัติของซอฟท์แวร์ป้องกัน ตรวจจับ และตอบสนองอัตโนมัติเครื่องผู้ใช้ปลายทาง (Endpoint Detection and Response) จำนวนไม่น้อยกว่า 10 ลิขสิทธิ์ ต้องมีคุณสมบัติขั้นต่ำหรืออย่างน้อย ดังต่อไปนี้

3.1 ป้องกัน Malware บนระบบปฏิบัติการได้ดังต่อไปนี้ Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, 2012 R2 Windows Server 2016, Windows Server 2019, Windows server 2022, MacOS และ Linux Ubuntu, Red Hat, Centos ได้

3.2 เป็นระบบ As a service เพื่อบริหารจัดการ โปรแกรมป้องกันไวรัสจากส่วนกลาง ผ่านทาง web console เดียวได้ทั้ง Endpoint, Workload และ XDR เป็นอย่างน้อย

3.3 ตรวจสอบ Malware แบบอ้างอิงจากฐานข้อมูล (Signature) และแบบวิเคราะห์พฤติกรรมอย่างน้อยดังนี้

3.3.1 Vulnerability Protection

3.3.2 Behavior Monitoring และ Ransomware Protection

3.3.3 Machine Learning และ Runtime Machine Learning

3.4 ป้องกันช่องโหว่ของระบบปฏิบัติการ โดยที่ไม่จำเป็นต้องทำการติดตั้ง patches บนระบบปฏิบัติการเหล่านั้นจริงได้ เพื่อป้องกันปัญหาที่อาจเกิดขึ้นจากการ patches โดยที่ยังไม่ได้ทำการทดสอบกับการใช้งานจริงได้ และเลือกนโยบายแบบ Recommended และ Aggressive ได้

3.5 ป้องกันข้อมูลสำคัญขององค์กรไม่ให้รั่วไหลออกไปภายนอกองค์กร (Data loss prevention) ผ่านทาง FTP, HTTP, Web Mail, Printer, Windows Clipboard, และ Removable Storage ได้ โดยใช้เงื่อนไขอย่างน้อยดังนี้ File Attributes, Keywords และ Regular Expressions

3.6 ป้องกันโปรแกรมประยุกต์ที่ไม่ได้รับอนุญาต (Lockdown, Block และ Allow) และไม่ต้องการให้ติดตั้งบนเครื่องคอมพิวเตอร์ลูกข่ายได้ (Application Control) และสามารถกำหนด Rule โดยใช้เงื่อนไขต่าง ๆ ได้

1.....ประธาน 2.....กรรมการ 3.....กรรมการและเลขานุการ

3.7 ป้องกัน ransomware ด้วยพฤติกรรม และสามารถกู้คืนไฟล์เอกสารที่ถูกโจมตีด้วย ransomware ได้

3.8 ป้องกันอันตรายที่มาจากทางเว็บไซต์ต่างๆ (Web Threats) ได้โดยใช้ Web Reputation ได้เป็นอย่างน้อย

3.9 ทำ Data loss prevention โดยมีความสามารถอย่างน้อยดังนี้

3.9.1 ตรวจสอบเนื้อหาในไฟล์ฟอร์แมตต่างๆ ในแบบ true file type เช่น Plain Text, Microsoft Office Documents(DOC, PPT, XLS), PDF ได้

3.9.2 แสดงรายละเอียดของผู้ละเมิด policy ได้อย่างน้อยเช่น Severity, Rule/Template, Endpoint, IP, Chanel, Email sender, Email subject, URLs, Action, File class และ User justification reason

3.10 ทำการค้นหาข้อมูลที่ละเอียดอ่อนขององค์กรว่าอยู่ที่ตำแหน่งใดบนเครื่องลูกข่าย (Endpoint) โดยใช้เงื่อนไข ได้ดังนี้

3.10.1 File Attributes

3.10.2 Keywords

3.10.3 Regular Expressions

3.11 กำหนดสิทธิ์การใช้งาน เช่น Full Access, Read, Read and Execute, Modify, List Content ให้กับอุปกรณ์ USB Storage devices ได้และสามารถอนุญาติให้ใช้งาน USB Storage ได้เป็นรายยี่ห้อ (Vendor ID) และ Serial Number ที่มีการลงทะเบียนในระบบเท่านั้น

3.12 กำหนดระดับการใช้งาน CPU ของเครื่องลูกข่ายระหว่างการ scan ได้

3.13 ข้ามการทำงานของ Scheduled Scan ได้โดยอัตโนมัติ หากว่าเครื่องลูกข่ายที่ใช้เป็นโน้ตบุ้คที่มีระดับไฟในแบตเตอรี่ต่ำกว่าที่กำหนด

3.14 หยุดการทำงานของ Scheduled Scan ได้โดยอัตโนมัติเมื่อใช้เวลาในการทำ Scan นานเกินกว่าที่กำหนด

3.15 ป้องกันไวรัสบนเครื่องลูกข่ายโดยป้องการการหยุดการทำงาน และถอดถอนการติดตั้ง โดยใช้รหัสผ่านได้

3.16 ป้องกันโปรแกรมประยุกต์ที่ไม่ได้รับอนุญาติและไม่ต้องการให้ติดตั้งไปยังเครื่องลูกข่ายได้ และกำหนด Rule โดยใช้เงื่อนไขได้ดังนี้

3.16.1 Application Reputation

3.16.2 File Path

3.16.3 Hash Values (SHA-1)

3.16.4 Certificate

3.16.5 Gray Software List

3.17 กำหนดนโยบายการอัพเดตให้เครื่องลูกข่ายที่กำหนดทำหน้าที่แจกจ่าย pattern ให้แก่เครื่องอื่นๆ ในมหาวิทยาลัย แทนที่เครื่องแม่ข่ายหลักได้ (Update Agent)

3.18 ต้องวิเคราะห์ และตอบสนองภัยคุกคามการตรวจจับแบบข้ามขั้น Extended detection and response (XDR) ได้

3.19 ต้องวิเคราะห์ และตอบสนองภัยคุกคามการตรวจจับแบบข้ามขั้น Extended detection and response (XDR) ต้องทำ response ทั้งแบบ Manual และ Automation(Security Playbooks) ในกรณีที่พบปัญหา โดยต้องทำได้อย่างน้อยดังนี้ Add Block List, Collect File, Isolate Endpoint และ Remote shell session

3.20 กำหนดสิทธิ์ของผู้ดูแลระบบในระดับที่แตกต่างกันด้วยสิทธิ์ที่ต่างกันได้ (User Role)

3.21 ออกรายงานการทำงานในรูปแบบ PDF, DOCX, และ XLSX ได้

3.22 ทำ MITRE ATT&CK mapping เพื่อช่วยให้เข้าใจสิ่งที่เกิดขึ้นบน Environment ได้อย่างรวดเร็ว พร้อม Hyperlinks ในการเชื่อมต่อไปยัง MITRE ATT&CK framework

1.....ประธาน 2.....กรรมการ 3.....กรรมการและเลขานุการ

3.23 ทำ Response หรือ Action หากเกิดภัยคุกคามเช่น Add to block list, Remove from Block list, Terminate, Collect file, Restore Message, Quarantine message, Delete message, Isolate endpoint, Restore connection และ Start remote shell session เป็นต้น

3.24 ทำ Execution Profile เพื่อวิเคราะห์ปัญหาต้นตอของภัยคุกคามที่เกิดขึ้น

3.25 มีระบบ Extended detection and response (XDR) รับ Activity ได้จากหลาย Product security ไม่เพียง Endpoint แต่ยังรวมถึง Email, workload, network, cloud เป็นต้น

3.26 เป็นแพลตฟอร์มเป็นลักษณะของ Software-as-a-Service ที่ hosted และ managed ผ่าน cloud

3.27 ทำการส่ง Syslog SIEM และ SOAR

3.28 เก็บบันทึกรายละเอียดกิจกรรม Activity ของเครื่อง Endpoint, Server, Network ได้แก่ DomainName, EndpointID, EndpointName, IPv4, IPv6, URL, Port, FileSHA1, FileFullPath, ProcessFullPath, CLICommand, RegistryKey, RegistryValue และ UserAccount

3.29 แบ่งปัน Suspicious Object ให้กับ Product อื่นๆ เพื่อเพิ่มการป้องกันภัยคุกคาม

3.30 สร้าง workbench ที่เมื่อมีการทริกเกอร์กับรูปแบบของการโจมตีโดยแสดงความเชื่อโยงทั้งหมดของเหตุการณ์ที่เกิดขึ้นโดยอัตโนมัติ

3.31 ทำงานร่วมกับระบบตรวจจับและวิเคราะห์ภัยคุกคามชั้นสูง (Sandbox as a Service)

3.32 ทำการเก็บข้อมูลหลักฐานต่างๆ ของเครื่องคอมพิวเตอร์ (Telemetry หรือ Forensic Analysis) เพื่อตรวจสอบเหตุการณ์การทำงานของมัลแวร์ (malware) ย้อนหลังได้ไม่น้อยกว่า 30 วัน โดยมีการเก็บข้อมูลไว้บนบริการที่ได้รับมาตรฐาน ISO 27001 เป็นอย่างน้อย

3.33 เพื่อป้องกันสินค้าลอกเลียนแบบ หรือสินค้าเก่านำมาใช้งานใหม่ ผู้เสนอราคาต้องได้รับการแต่งตั้งเป็นตัวแทนจำหน่าย จากบริษัทผู้ผลิต หรือสาขาของผู้ผลิต หรือตัวแทนจำหน่ายในประเทศ

3.34 ต้องมีทีม support เพื่อรองรับบริการหลังการขาย

4. เงื่อนไขทั่วไป

4.1 ติดตั้งและส่งมอบที่สำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ กรุงเทพมหานคร

4.2 รับประกันเป็นเวลาอย่างน้อย 1 ปี

4.3 กำหนดส่งมอบภายใน 120 วันนับถัดจากวันลงนามในสัญญา

4.4 ผู้เสนอราคาต้องแนบเอกสารข้อกำหนดคุณลักษณะ ซึ่งตรงหรือดีกว่า ที่กำหนดไว้ในเอกสารนี้โดยต้องแนบแคตตาล็อกของผลิตภัณฑ์ที่เสนอ โดยความสามารถของผลิตภัณฑ์ต้องทำได้ ณ วันเสนอราคา และแคตตาล็อกต้องเป็นเอกสารจากผู้ผลิต โดยระบุยี่ห้อ และรุ่นที่เสนอราคาอย่างชัดเจนประกอบการเสนอราคา

4.5 ผู้เสนอราคาต้องจัดทำตารางเปรียบเทียบข้อกำหนดคุณลักษณะเฉพาะครุภัณฑ์ของมหาวิทยาลัยกับครุภัณฑ์ที่เสนอ โดยอ้างอิงถึงหัวข้อและหน้าของเอกสาร

1.....ประธาน 2.....กรรมการ 3.....กรรมการและเลขานุการ