ความเป็นมาของโซลูชั่นที่นำเสนอ

การนำระบบเทคโนโลยีสารสนเทศเข้ามาประยุกต์ใช้งานภายในองค์กรส่งผลให้เกิดการพัฒนาแบบก้าวกระโดดแก่องค์กร ทั้งในแง่ของประสิทธิภาพและประสิทธิผลที่เกิดขึ้นไม่ว่าจะเป็น การขับเคลื่อนวิสัยทัศน์และพันธกิจขององค์กร การปฏิบัตงานของเจ้าหน้าที่ภายในองค์กร รวมไปถึงการให้บริการแก่ภาคประชาชน แต่สิ่งที่มาพร้อมกับเทคโนโลยีนั่นคือ ภัยคุกคามทางด้านไซเบอร์ที่ปัจจุบันเพิ่มขึ้นอย่างรวดเร็ว ด้วยวิธีการหลากหลายรูปแบบ มีความซับซ้อนมากขึ้นและมีวัตถุประสงค์ที่แตกต่างกันไปไม่ว่าจะเป็นการทำลายระบบ (Destroy) การขโมยข้อมูล (Data Theft) การหลอกลวง (Phishing) และการเรียกค่าไถ่ (Ransomware) ซึ่งภัยคุกคามทางด้านไซเบอร์เหล่านี้ ได้สร้างความเสียหายและทำลายความมั่นคงต่อระบบเทคโนโลยีสารสนเทศขององค์กร ส่งผลกระทบโดยตรงต่อการดำเนินงานให้สอดคล้องกับวิสัยทัศน์และพันธกิจขององค์กร การปฏิบัติของเจ้าหน้าที่ และผู้ใช้บริการในภาคประชาชน

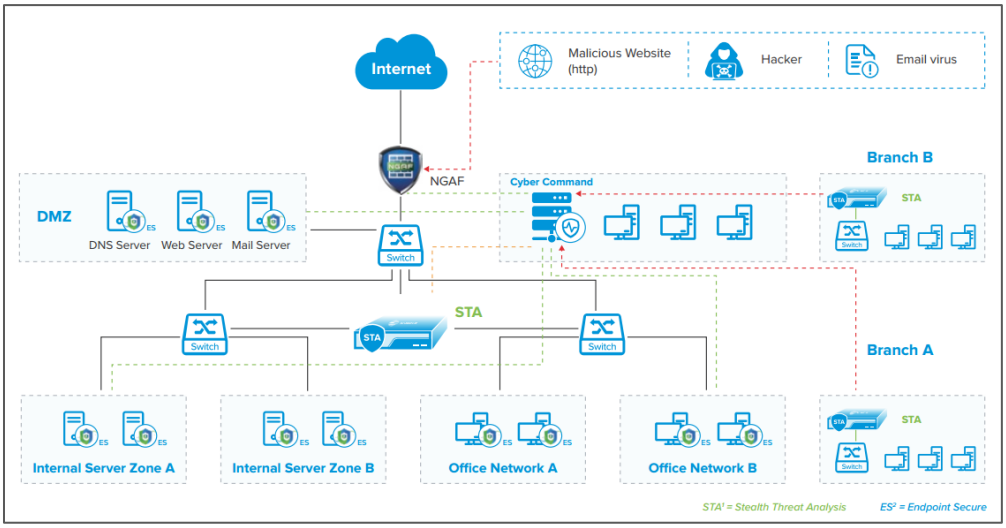
อย่างไรก็ตามถึงแม้องค์กรจะมีการนำระบบหรืออุปกรณ์รักษาความปลอดภัยทางด้านไซเบอร์เข้ามาใช้งานภายในองค์กรเพื่อป้องกันและปกป้องระบบเทคโนโลยีสารสนเทศจากภัยคุกคามทางด้านไซเบอร์ตามหลักการความมั่นคงปลอดภัยทางไซเบอร์ แต่กลับพบว่าระบบหรืออุปกรณ์รักษาความปลอดภัยทางด้านไซเบอร์แบบเดิม (Traditional Cyber Security) ไม่ว่าจะเป็น Endpoint Security, Network Security รวมไปถึงระบบ SIEM ที่ยังมีข้อจำกัดทางด้านความสามารถหรือศักยภาพในการทำงานร่วมกันซึ่งไม่เพียงพอต่อการเฝ้าระวัง วิเคราะห์ ตรวจจับ และตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ที่เกิดขึ้นได้ ทำให้องค์กรจำเป็นต้องมีการปรับปรุงหรือเพิ่มเติมระบบรักษาความปลอดภัยทางด้านไซเบอร์ให้มีความทันสมัยมากขึ้นสามารถทำงานร่วมกันเพื่อการตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ที่เกิดขึ้นได้อย่างมีประสิทธิภาพ

บริษัท ซังฟอร์ เทคโนโลยี ประจำประเทศไทย (Sangfor Technologies Thailand Co., Ltd) มีความยินดีในการนำเสนอ **“ระบบอัจฉริยะสำหรับการตรวจจับ และตอบสนองต่อภัยคุกคามทางด้านไซเบอร์ (Intelligent Threat Detection and Response Platform)”** ซึ่งเป็นการปรับปรุงระบบรักษาความปลอดภัยทางด้านไซเบอร์แบบเดิม (Traditional Cyber Security) ให้มีความทันสมัยมากขึ้นเพื่อให้สามารถรับมือกับภัยอาชญากรรมและภัยคุกคามทางด้านไซเบอร์ได้อย่างเต็มประสิทธิภาพสูงสุด

วัตถุประสงค์ของการนำเสนอโซลูชั่น

1. เพื่อปรับปรุงระบบรักษาความปลอดภัยทางด้านไซเบอร์ขององค์กรให้มีประสิทธิภาพดีขึ้น
2. เพื่อใช้เป็นเครื่องมือสำหรับเพิ่มประสิทธิภาพในการปฏิบัติงานให้กับผู้ดูแลระบบ
3. เพื่อช่วยลดความเสี่ยงและผลกระทบจากภัยคุกคามทางด้านไซเบอร์ที่จะส่งผลต่อการดำเนินงานหรือธุรกิจขององค์กร

ภาพรวมการทำงานของระบบ



รูปภาพที่ 1 ภาพรวมการทำงานของระบบ Intelligent Threat Detection and Response Platform

ความสามารถของแต่ละผลิตภัณฑ์ในระบบ

ผลิตภัณฑ์	รายละเอียดด้านความสามารถของผลิตภัณฑ์
Cyber Command (CCOM) Intelligent Threat Detection and Response	ทำหน้าที่ในการรับหรือรวบรวมข้อมูลจากผลิตภัณฑ์ต่างๆ ของซังฟอร์ ได้แก่ Stealth Threat Analysis (STA), Next Generation Application Firewall (NGAF), Endpoint Secure (ES) และ Neural-X Cloud Threat Intelligence โดยมีการนำระบบปัญญาประดิษฐ์ (AI) มาใช้เพื่อเพิ่มประสิทธิภาพความเร็วและความแม่นยำในการสร้างความสัมพันธ์ของข้อมูลเพื่อใช้ในการ ตรวจจับ ภัยคุกคามต่างๆที่มีความซับซ้อนและเกิดขึ้นภายในระบบเครือข่ายขององค์กร หรือการแพร่กระจายของมัลแวร์ภายในระบบเครือข่ายทำให้สามารถตีกรอบในการแก้ปัญหาได้รวดเร็วยิ่งขึ้น (Detection) ในกรณีที่มีการใช้งาน Sangfor Next Generation Application Firewall (NGAF) และ Endpoint Secure (ES) ร่วมด้วย สามารถส่งคำสั่งจากอุปกรณ์ Cyber Command ไปยังผลิตภัณฑ์ทั้ง 2 ตัวเพื่อทำการ Scan Malware หรือ Kill Malicious Process และทำการ Block Malicious Traffic ได้ทันที (Response) **หมายเหตุ หากไม่มีการใช้งาน NGAF และ ES อุปกรณ์สามารถทำการ Detection & Reporting ได้**

Stealth Threat Analysis (STA)	ทำหน้าที่ในการรับข้อมูลเน็ตเวิร์คทราฟฟิค (Network Traffic) ผ่านอุปกรณ์ Core Switch ด้วยวิธีการ SPAN/Mirror Port เพื่อนำมาใช้ในการวิเคราะห์ภัยคุกคามหรือตรวจสอบพฤติกรรรมผิดปรกติ ที่เกิดขึ้นภายในระบบเครือข่ายขององค์กร และทำการส่งผลลัพธ์ที่ได้ไปยังอุปกรณ์ Cyber Command เพื่อใช้ในการทำ Threat Detection and Response ต่อไป
Next Generation Application Firewall (NGAF)	ทำหน้าในการควบคุมการใช้งานอินเตอร์เน็ตของผู้ใช้งานและป้องกันภัยคุกคามทางด้านไซเบอร์จากทั้งภายนอก (Outsider Threat) ที่จะเข้ามาโจมตีระบบคอมพิวเตอร์หรือระบบเครือข่ายขององค์กร ยกตัวอย่างเช่น Phishing, Web Attack เป็นต้น โดยมีการนำระบบปัญญาประดิษฐ์ (AI) มาใช้เพื่อเพิ่มประสิทธิภาพความเร็วและความแม่นยำในการตรวจสอบและวิเคราห์ที่สูงขึ้น สามารถทำงานร่วมกับ Cyber Command โดยการรับคำสั่งจาก Cyber Command เพื่อทำการ Block Malicious Traffic จากเครื่องคอมพิวเตอร์ภายในองค์กรที่ติดมัลแวร์ (Compromised) และพยายามที่จะติดต่อไปยังเครื่องแม่ข่ายของแฮคเกอร์หรือที่เรียกว่า Command & Control Server ได้ทันที
Endpoint Secure (ES)	ทำหน้าที่ในการป้องกันมัลแวร์ต่างๆ (Malware) ที่จะเข้ามาโจมตีระบบเครื่องคอมพิวเตอร์ของผู้ใช้งานและระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการผู้ใช้งาน โดยมีการนำระบบปัญญาประดิษฐ์ (AI) มาใช้เพื่อเพิ่มประสิทธิภาพความเร็วและความแม่นยำในการตรวจสอบและวิเคราห์ที่สูงขึ้น สามารถทำงานร่วมกับ Cyber Command โดยการรับคำสั่งจาก Cyber Command เพื่อทำการ Scan Malware หรือ Kill Malicious Process จากเครื่องคอมพิวเตอร์ภายในองค์กรที่ติดมัลแวร์ (Compromised) ได้ทันที
Neural-X (Cloud Threat Intelligence)	ทำหน้าที่รวบรวมภัยคุกคามทางด้านไซเบอร์ต่างๆที่เกิดขึ้นจากทั่วทุกมุมโลก และทำการอัพเดทข้อมูลดังกล่าวมายังทุกผลิตภัณฑ์ของ Sangfor เพื่อใช้เป็นข้อมูลในการวิเคราะห์ตรวจจับ และป้องกันหรือตอบสนองต่อภัยคุกคามที่เกิดขึ้นภายในองค์กร

แนะนำผลิตภัณฑ์ Cyber Command

ผลิตภัณฑ์ Cyber Command คือโซลูชั่นที่นำมาแก้ปัญหาในเรื่องของการตรวจจับและตอบสนองต่อภัยคุกคามที่เกิดขึ้นภายในองค์กร (Insider Threat) จากข้อจำกัดของเทคโนโลยีตรวจจับภัยคุกคามแบบเดิม (Traditional Security Solution) ภายใต้หลักการทำงานที่เรียกว่า Intelligent Detection and Response โดยมีขั้นตอนการทำงานด้วยกันทั้งหมด 3 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 การตรวจจับภัยคุกคาม (Threat Detection)

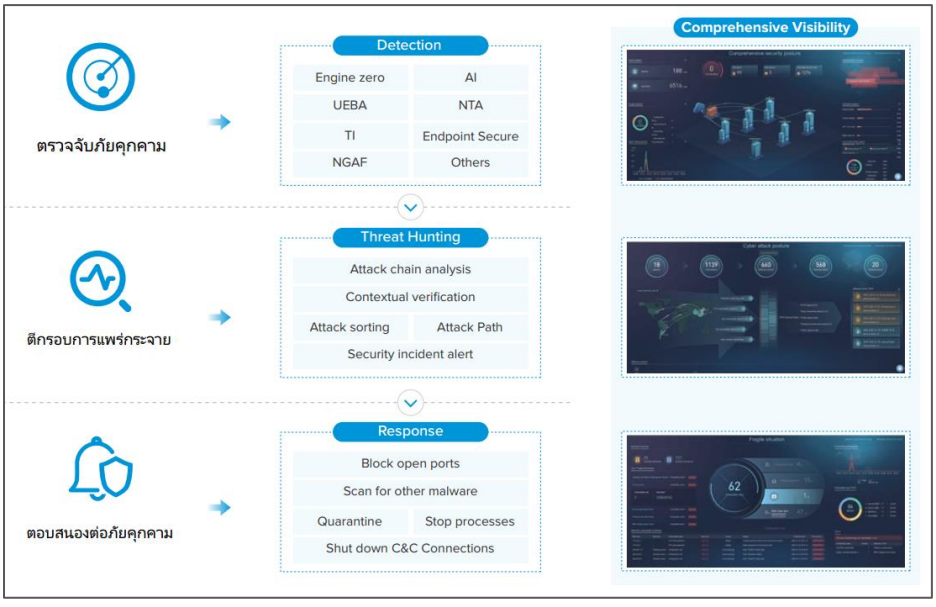
ทำการเก็บรวบรวมข้อมูลในระบบเครือข่าย (Network Traffic Analytic) และผลิตภัณฑ์ด้าน Cyber Security อื่นๆของ Sangfor ได้แก่ Endpoint Secure, Next Generation Application Firewall และ Cloud Threat Intelligence นำมาใช้ในการวิเคราะห์และสร้างความสัมพันธ์ของภัยคุกคาม (Threat) หรือพฤติกรรมการใช้งานที่ผิดปรกติ (UEBA) ที่เกิดขึ้นในระบบเครือข่าย

ขั้นตอนที่ 2 การตีกรอบการแพร่กระจายของภัยคุกคาม (Threat Hunting)

ทำการตีกรอบการแพร่กระจายของมัลแวร์ภายในระบบเครือข่าย รวมไปถึงสถานะการโจมตีและความเสี่ยงที่เกิดขึ้นจากเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ (Stage of Chain Attack) ทำให้แก้ปัญหาได้ตรงจุด สามารถลดผลกระทบและความเสียหายที่เกิดขึ้นได้อย่างมีประสิทธิภาพ

ขั้นตอนที่ 3 การตอบสนองต่อภัยคุกคามที่เกิดขึ้น (Threat Response)

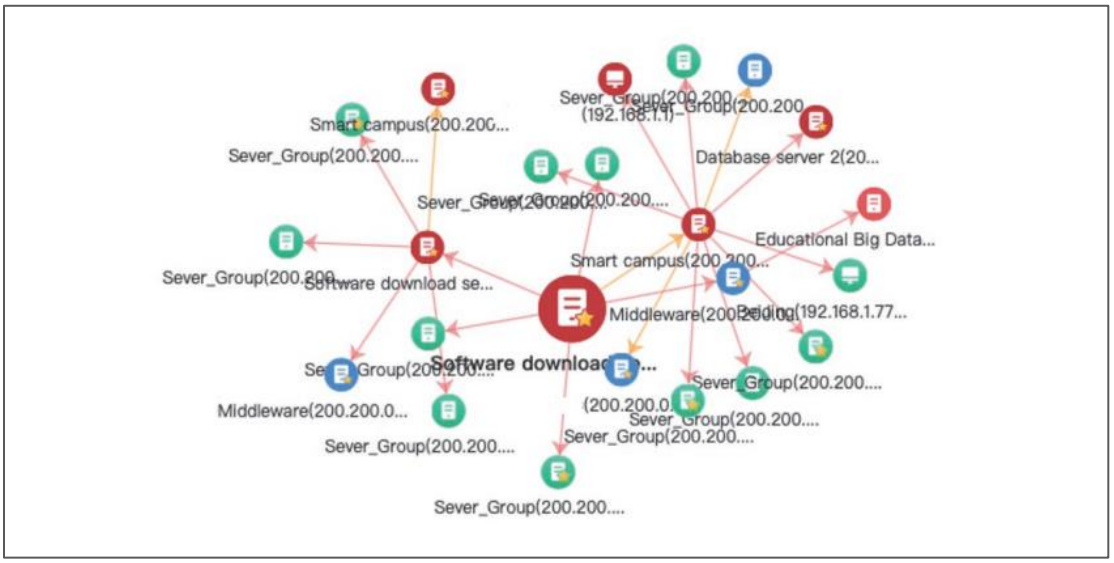
มีรายงานสรุปพร้อมแนวทางหรือวิธีการในการตอบสนองต่อภัยคุกคามที่เกิดขึ้น และในกรณีที่มีการใช้งานผลิตภัณฑ์ Cyber Security ของ Sangfor ได้แก่ Endpoint Secure และ Next Generation Application Firewall สามารถส่งคำสั่งจากอุปกรณ์ Cyber Command เพื่อทำการ Scan Malware หรือ Kill Malicious Process และทำการ Block Malicious Traffic ได้ทันที



รูปภาพที่ 2 ภาพรวมการทำงานของอุปกรณ์ Cyber Command

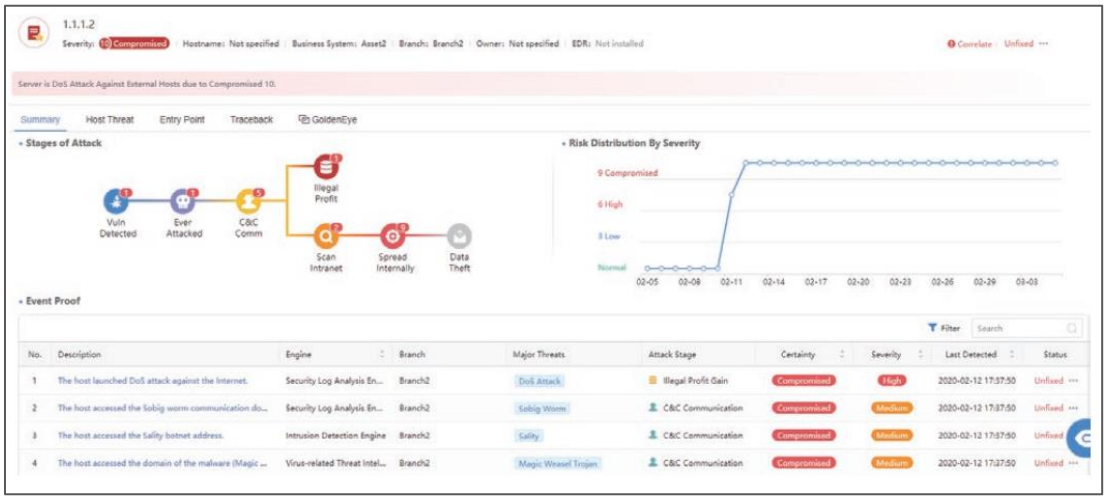
แนะนำความสามารถที่สำคัญของผลิตภัณฑ์ Cyber Command

1. Golden Eye คือความสามารถในการทำ Threat Hunting ของอุปกรณ์ Cyber Command โดยการสร้างความสัมพันธ์ของเครื่องคอมพิวเตอร์ที่มีความเสี่ยงจากภัยคุกคามร่วมกัน และแสดงผลลัพธ์ออกมาในรูปแบบของ Topology Visualization เพื่อให้ง่ายต่อการตรวจสอบ



รูปภาพที่ 3 การทำ Threat Hunting ด้วยความสามารถของ Golden Eye ในอุปกรณ์ Cyber Command

2. Stage of Attack Chain ทำให้ทราบระดับความรุนแรง (Severity) ของเครื่องคอมพิวเตอร์ที่ถูกโจมตี (Host Compromised) ว่าอยู่ในขั้นตอนใด มีความเสี่ยงหรือความรุนแรงมากน้อยแค่ไหน เพื่อให้ง่ายต่อการ ประเมินความเสี่ยงและจัดลำดับความสำคัญก่อนหลังในการแก้ปัญหาได้มีประสิทธิภาพยิ่งขึ้น



รูปภาพที่ 4 การทำ Chain Attack Status เพื่อให้ทราบความเสี่ยงที่เกิดขึ้นจากเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ (Host Compromised)

3. หน้าจอ Dashboard สำหรับการทำ SOC Monitoring หรือ Cyber War Room ช่วยทำให้ผู้ดูแลระบบเข้าใจสถานะภาพรวมภัยคุกคามที่เกิดขึ้นกับองค์กรแบบ 360 องศาทั้งภัยคุกคามที่เกิดขึ้นจากภายนอก (Inbound Attack) และภัยคุกคามที่เกิดขึ้นจากภายใน (Outbound Attack) โดยข้อมูลเหล่านี้จะช่วยให้ผู้ดูแลระบบสามารถใช้ในการประเมินและตัดสินใจในการดำเนินการป้องกันได้ง่ายยิ่งขึ้น

รูปภาพที่ 5 SOC Dashboard สำหรับแสดงภัยคุกคามที่มีการโจมตีเข้ามาในระบบขององค์กรจากภายนอก (Inbound Attack)

รูปภาพที่ 6 SOC Dashboard สำหรับแสดงภัยคุกคามที่ระบบคอมพิวเตอร์ขององค์กรถูกใช้เป็นฐานโจมตีผู้อื่น (Outbound Attack)

ประโยน์ที่จะได้รับจากการใช้งานผลิตภัณฑ์ Cyber Command

รูปภาพที่ 7 ประโยชน์ที่จะได้รับจากการใช้งานผลิตภัณฑ์ Cyber Command

ผลลัพธ์ที่ได้จากการใช้งานโซลูชั่น

1. เป็นการยกระดับระบบรักษาความปลอดภัยทางด้านไซเบอร์ให้มีความทันสมัย สามารถรับมือกับภัยอาชญากรรมและภัยคุกคามทางด้านไซเบอร์ที่มีความซับซ้อนได้อย่างเต็มประสิทธิภาพสูงสุด
2. ลดความเสี่ยงและผลกระทบจากภัยคุกคามทางด้านไซเบอร์ที่จะส่งผลต่อการดำเนินงานหรือธุรกิจขององค์กร พร้อมทั้งรองรับนโยบาย Thailand ๔.๐ เพื่อให้การบริการระบบงานสารสนเทศต่างๆ เป็นไปได้อย่างต่อเนื่อง
3. ช่วยเพิ่มประสิทธิภาพและประสิทธิผลให้กับระบบรักษาความปลอดภัยทางด้านไซเบอร์เพื่อให้สอดคล้องกับ พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์, พรบ. คุ้มครองข้อมูลส่วนบุคคล และ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

บทสรุปเกี่ยวกับบริษัทซังฟอร์ เทคโนโลยี (Sangfor Technologies Inc.)

บริษัท Sangfor Technologies Inc. ก่อตั้งขึ้นในปี พ.ศ. 2543 เป็นบริษัทที่ให้บริการโซลูชั่นโครงสร้างพื้นฐานไอทีในประเทศจีนและในระดับสากล มีความเชี่ยวชาญในการจัดหาระบบคลาวด์คอมพิวติ้งและโซลูชั่นการรักษาความปลอดภัยทางด้านไซเบอร์และการเพิ่มประสิทธิภาพให้กับระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายภายในองค์กร มีสำนักงานสาขาประจำประเทศไทย โดยจดทะเบียนบริษัทภายใต้ชื่อบริษัท Sangfor Technologies (Thailand) Co., Ltd ก่อตั้งขึ้นในปี พ.ศ. 2553 ปัจจุบันมีพนักงานประจำประเทศไทยทั้งหมด 14 คน

<u>เอกสารแนบท้ายเพิ่มเติมสำหรับโซลูชั่นที่นำเสนอ</u>

1. Cyber Command Intelligent Threat Detection and Response Platform
2. Endpoint Protection and Response Platform
3. NGAF Next Generation Firewall