Hillstone NETWORKS

I-Series

Network Traffic Analysis (NTA)

Network Traffic Analysis (NTA) หรือ การวิเคราะห์การใช้งานของ Network Traffic ภายในเครือข่าย

การวิเคราะห์ข้อมูล traffic ในเครือข่าย (NTA) ล่าสุดจาก Gartner โดยกำหนดหมวดหมู่ความปลอดภัยขึ้นใหม่ซึ่งใช้การสื่อสารเครือข่ายเป็นแหล่งข้อมูลพื้นฐานสำหรับตรวจจับภัยคุกคามและความผิดปกติที่เกิดขึ้นภายในเครือข่าย

NTA ได้รับเลือกให้เป็นหนึ่งใน 11 เทคโนโลยีที่เกิดขึ้นใหม่ในปี 2560 โดย Gartner ในขณะที่เทคโนโลยีกำลังเติบโต

เมื่อวันที่ 28 กุมภาพันธ์ 2019 Gartner ตีพิมพ์คู่มือการตลาดครั้งแรกสำหรับ NTA ในรายงานนี้ได้มีการนำเสนอภาพรวมของเทคโนโลยี NTA, กำหนดทิศทางการตลาด, และวิเคราะห์ผลิตภัณฑ์ที่เกี่ยวข้องจากผู้ผลิตชั้นนำ ซึ่งรวมถึง HillStone Breach Detection System ในรายงานนี้ด้วย

NTA คืออะไร

เทคโนโลยี NTA นั้นมีมาระยะหนึ่งแล้ว และใช้งานกันอย่างแพร่หลายในการตรวจสอบเครือข่ายและการวิเคราะห์ปริมาณการใช้งานครือข่ายทั้งหมดได้อย่างครอบคลุมเพื่อทราบถึงข้อมูลเชิงลึกภายในเครือข่าย

ตามที่ปรากฏในทุกวันนี้ อาชญากรไซเบอร์, แฮ็กเกอร์ ทั้งมือสมัครเล่นและมืออาชีพกำลังใช้เทคนิค และเครื่องมือขั้นสูง ในการโจมตีทางไซเบอร์ การโจมตีเหล่านี้มีการกำหนดเป้าหมายที่ชัดเจน, มีความซับซ้อน และเป้าหมายของพวกเขามักเกี่ยวข้องกับการขโมยข้อมูลของผู้ใช้ (user credentials), และข้อมูลสำคัญทางธุรกิจ เทคโนโลยีในการตรวจจับ และป้องกันภัยคุกคามแบบเดิม เช่น Signature-based ไม่เพียงพอที่จะตรวจจับ และป้องกันการโจมตีที่ซับซ้อนเหล่านี้

NTA ใช้เทคนิคการวิเคราะห์ที่ขับเคลื่อนโดย AI และ machine learning ในการตรวจจับภัยคุกคามรูปแบบใหม่ที่มีความหลากหลาย และได้รับการพิสูจน์แล้วว่ามีประสิทธิภาพในการตรวจจับการโจมตีขั้นสูง

NTA สามารถสร้างพื้นฐานการรับส่งข้อมูล (Baseline) และใช้พื้นฐานนั้นเพื่อแสดงรูปแบบการรับส่งข้อมูลปกติและพฤติกรรมของแอพพลิเคชั่นที่เกิดขึ้นภายในเครือข่าย ยิ่งไปกว่านั้น สิ่งเหล่านี้ยังแสดงถึงพฤติกรรมปกติและไม่ปกติของผู้ใช้ที่เข้าถึงแอพพลิเคชั่น และบริการต่างๆที่มีการใช้งานบนระบบเครือข่าย

เมื่อมีการสร้าง baselines ขึ้นมา การรับส่งข้อมูลเครือข่ายจะถูกวิเคราะห์ตาม algorithms ทางคณิตศาสตร์ หรือ machine learning algorithms โดยสามารถวิเคราะห์รูปแบบการรับส่งข้อมูลและการเรียกใช้แอพพลิเคชั่นที่ผิดปกติ และสามารถนำเสนอผลการวิเคราะห์ที่ครอบคลุมให้กับนักวิเคราะห์ด้านความปลอดภัยและผู้ดูแลระบบได้เพื่อดำเนินการกับความผิดปกติที่ระบบ NTA แจ้งเตือนและลดความเสียหายที่อาจเกิดขึ้นต่อองค์กร

แพลตฟอร์ม NTA ประกอบด้วยองค์ประกอบสำคัญเหล่านี้

Traffic Collector : ระบบรวบรวมข้อมูล network traffic

Traffic ชนิดต่างๆ ในเครือข่าย เช่น log traffic และ pcaps จะถูกรวบรวม, คัดแยก, วิเคราะห์, และส่งต่อไปยังโมดูลจัดเก็บข้อมูล ตัวเก็บรวบรวม traffic มักจะถูกปรับใช้ในโหมด tapping เพื่อลดผลกระทบต่อการใช้งานเครือข่าย

Traffic Data Storage : ระบบจัดเก็บข้อมูล network traffic

Data จะถูกจัดเก็บในฐานข้อมูล ทั้งแบบ centralized หรือแบบกระจาย โดยผู้ใช้สามารถ query และค้นหา Traffic log หรือ metadata ได้อย่างยืดหยุ่นและมีประสิทธิภาพ โดยทั่วไปแล้วข้อมูลจะถูกเก็บไว้เป็นระยะเวลานาน ซึ่งสามารถใช้สำหรับตรวจจับภัยคุกคาม การสืบค้น และการพิสูจน์หลักฐาน

Traffic Analysis Engine : ระบบวิเคราะห์ network traffic

NTA สามารถวิเคราะห์ network traffic ได้หลากหลายรูปแบบซึ่งสามารถใช้ได้ตั้งแต่การวิเคราะห์ทางสถิติอย่างง่าย ไปจนถึง algorithm ของ machine learning ที่ซับซ้อน เป้าหมายคือการระบุแอพพลิเคชั่นและบริการที่มีรูปแบบ traffic เกินกว่าเกณฑ์ที่ได้รับจาก baseline ที่จัดตั้งขึ้น

Output Module : ระบบแสดงผล

เมื่อมีการ generate ผลลัพธ์ของ traffic analysis, log, และ alert แล้ว ผลลัพธ์นั้นจะปรากฏใน user interface สำหรับนักวิเคราะห์ด้านความปลอดภัยและผู้ดูแลระบบ เพื่อดำเนินการที่เหมาะสม เช่น การนำไปใช้ทำนโยบายบน firewall เพื่อปิดกั้นโฮสต์ที่น่าสงสัย หรือควบคุม traffic ที่เกี่ยวข้องกับโฮสต์ที่ถูกโจมตี

เทคโนโลยี NTA มีความสำคัญต่อความปลอดภัยในโลกไซเบอร์ เป็นเครื่องมือที่มีประสิทธิภาพในการรับข้อมูลเชิงลึกของ traffic ในเครือข่ายและปริมาณการใช้งานแอพพลิเคชั่นแบบ real time โดยเฉพาะการรับส่งข้อมูลภายในเครือข่าย (East-West Traffic) ซึ่งเป็น การรับส่งข้อมูลภายในเครือข่ายที่ไม่ผ่าน gateway และมักจะเกี่ยวข้องกับการเคลื่อนไหวระหว่าง Vlan หรือ lateral movement เป็นการตรวจจับภัยคุกคามเมื่อเกิดการละเมิดนโยบายเครือข่ายขององค์กร รวมถึงกิจกรรมที่ไม่ได้รับอนุญาตภายในเครือข่าย

Hillstone BDS ช่วยให้คุณเข้าใจและดำเนินการ วิเคราะห์ network traffic

ในคู่มือการตลาด NTA ของ Gartner ระบบ Breach Detection System (BDS) จาก Hillstone Networks ได้รับเลือกจาก Gartner ให้เป็นผลิตภัณฑ์ชั้นนำหลังจากได้รับการรีวิวอย่างละเอียด

Hillstone BDS ใช้ multiple engine เพื่อตรวจจับภัยคุกคาม เช่น Intrusion Prevention System (IPS) และ Machine Learning Algorithm รวมถึง Layer 7 Traffic Metadata เพื่อสร้าง baseline ในโหมดการเรียนรู้โดยไม่ต้องถอดรหัสการรับส่งข้อมูล SSL / TLS แบบ real time การใช้ algorithm ทางคณิตศาสตร์ขั้นสูงเพื่อระบุความเบี่ยงเบนจากกิจกรรมปกติจะสามารถตรวจพบกิจกรรมที่ผิดปกติได้ Hillstone BDS สามารถทำงานร่วมกับ Hillstone Next Generation Firewalls เพื่อเพิ่มความ สามารถในการบล็อก Threats ที่ตรวจจับได้แบบอัตโนมัติ

โซลูชั่น NTA ของ Hillstone เป็นส่วนหนึ่งของแพลตฟอร์มการรักษาความปลอดภัย และช่วยบริหารจัดการความเสี่ยงขององค์กร ด้วยการปกป้องแบบ layered protection ที่ช่วยให้องค์กรสามารถตรวจสอบพฤติกรรมของผู้ใช้และแอพพลิเคชันที่ผิดปกติภายในเครือข่ายได้อย่างละเอียด

สอบถามข้อมูลเพิ่มเติมได้ที่ บริษัท บลูซีบรา จำกัด
9/66 ถนนรัชดาภิเษก แขวงจตุจักร เขตจตุจักร กรุงเทพ 10900
โทร: (02) 587-9881 FAX: (02) 587-9882 www.bluezebra.co.th