NetGain Security Analytics Datasheet

แนวทางในการรักษาความปลอดภัยด้านไอที มีการพัฒนาอยู่ตลอดเวลา เราได้ยกระดับจากการรักษาความปลอดภัยภายในขอบเขตองค์กร (perimeter security) ไปสู่ความปลอดภัยทางไซเบอร์ (Cybersecurity) ตั้งแต่การปกป้องเฉพาะทรัพย์สินขององค์กร ไปจนถึงการรับรองความปลอดภัยของอุปกรณ์ทรัพย์สินและข้อมูลของผู้ใช้ และอุปกรณ์ IoT ที่เชื่อมต่อกับเครือข่ายขององค์กร

ในขณะที่องค์กรต่างๆ อาจลงทุนในโซลูชันด้านความปลอดภัย เช่น ไฟร์วอลล์และซอฟต์แวร์ตรวจจับมัลแวร์ แต่ในที่สุดก็ยังไม่มีทางรับประกันได้ 100% ว่าแฮ็กเกอร์จะไม่สามารถเจาะเข้าระบบเครือข่ายขององค์กรได้ เช่นนี้แผนกไอทีจึงมีความจำเป็นอย่างยิ่ง ที่ต้องหันมาหาโซลูชั่น SIEM (Security Information and Event Management) มากขึ้นเรื่อยๆ เพื่อตรวจจับพฤติกรรมที่ผิดปกติและภัยคุกคามที่อาจเกิดขึ้นภายในองค์กร

ด้วยการวิเคราะห์ข้อมูล log จากหลายแหล่งในโครงสร้างพื้นฐานด้านไอที ที่สร้างขึ้นโดยเหตุการณ์และกิจกรรมต่างๆ SIEM จะสามารถระบุภัยคุกคามดังกล่าว ตามเวลาจริงและแจ้งเตือนทีมปฏิบัติการด้านความปลอดภัยที่เกี่ยวกับภัยคุกคามดังกล่าว

SIEM เป็นเครื่องมือที่มีประโยชน์สำหรับการพิสูจน์หาหลักฐาน ตรวจสอบค้นหาจากข้อมูลในอดีตเพื่อระบุหลักฐานการโจมตีหรือรูปแบบการโจมตีที่ผ่านมา

NetGain Security Analytics

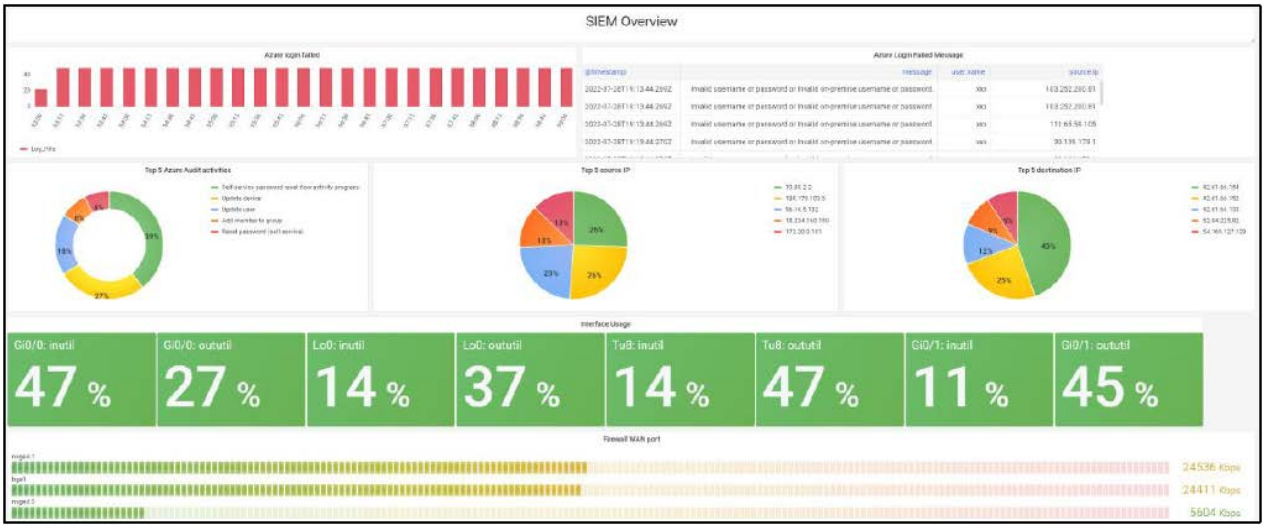
การใช้งานโซลูชัน NetGainSIEM ไม่ได้เป็นเรื่องที่ซับซ้อนและมีค่าใช้จ่ายสูงเหมือนกับโซลูชัน SIEM อื่นๆ NetGain Security Analytics จะปรับมุมมองทางด้านการมองเห็นภาพรวมขององค์กรของคุณเรื่องความปลอดภัย และระบุภัยคุกคามต่อโครงสร้างพื้นฐานด้านไอทีของคุณ โดยเชื่อมโยงเหตุการณ์ต่างๆ จาก log ข้อมูลที่เป็นภัยคุกคาม

ไม่เหมือนกับโซลูชัน SIEM อื่นๆ ส่วนใหญ่ NetGain Security Analytics สามารถช่วยลดความยุ่งยากในการปรับใช้ SIEM เพื่อเข้าถึงองค์กรที่มีแผนกไอทีขนาดเล็ก เช่นเดียวกันยังมีความยืดหยุ่น มีความสามารถในการปรับเปลี่ยนขนาดที่เหมาะสมกับองค์กรขนาดใหญ่ ที่มีความต้องการมากขึ้น แต่ต้องการลดความซับซ้อน ในการจัดการการดำเนินงานความปลอดภัยด้านไอที

โซลูชัน NetGain Security Analytics ประกอบด้วยฟังก์ชันดังนี้

- Log Analytics: การนำเข้าบันทึก ความสามารถในการค้นหาที่มีประสิทธิภาพ watcher และ Report
- Security Analytic: การวิเคราะห์ความปลอดภัย ซึ่งให้ความสามารถในการตามล่าภัยคุกคามด้านความปลอดภัย (security threat hunting)

NetGain Security Analytics มีให้บริการทั้งแบบซอฟต์แวร์ภายในองค์กร on-premise หรือแบบ SaaS



Key Features

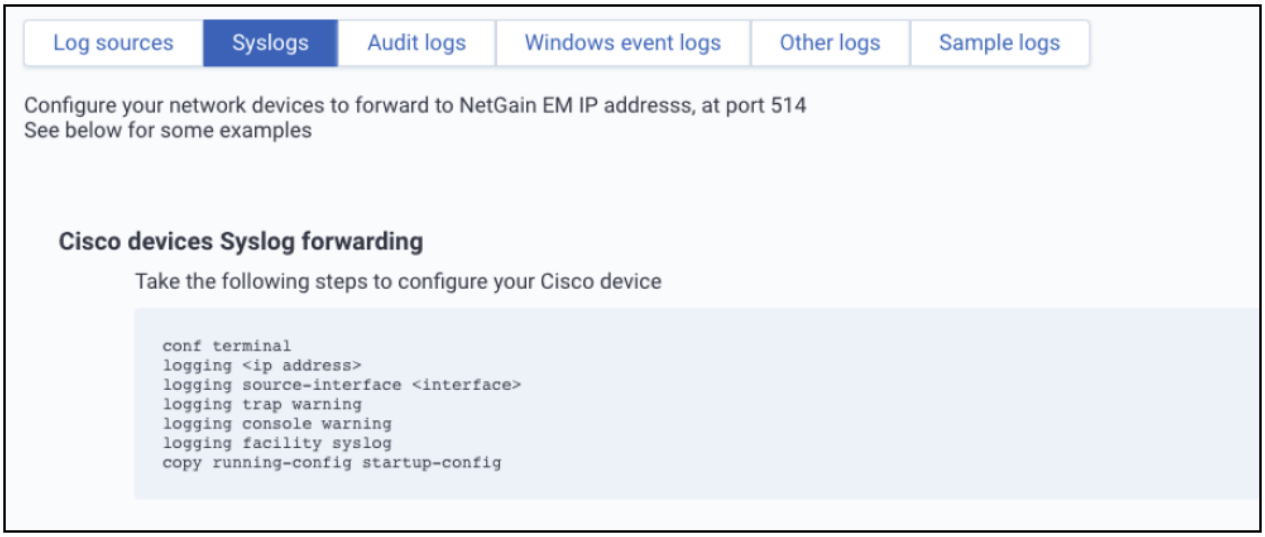
Log Analytics

Log Analytics ได้รับการออกแบบมาเพื่อรวบรวมข้อมูล log จากอุปกรณ์ IT ต่างๆ อุปกรณ์ Security, Servers, Networks และอื่นๆ ไม่ว่าจะอยู่ในองค์กรหรือในระบบคลาวด์ log ถูกจัดเตรียมรูปแบบ (mapped) ซึ่งจะช่วยให้สามารถค้นหาและเชื่อมโยงได้อย่างชาญฉลาด ผู้ใช้งานสามารถสร้างแดชบอร์ดที่กำหนดเองและรายงานกได้จากข้อมูล log

- Comprehensive log sources supported

รองรับแหล่งที่มาของข้อมูล log ที่หลากหลาย รวมถึง syslogs จากเครือข่าย อุปกรณ์รักษาความปลอดภัย เซิร์ฟเวอร์ ภายในองค์กรและระบบคลาวด์

คำแนะนำเกี่ยวกับวิธีกำหนดค่าอุปกรณ์เพื่อส่งบันทึกไปยัง NetGain



- Efficient log mapping using Filebeat and GROK

การจัดรูปแบบข้อมูล log (mapping) เป็นกระบวนการนำข้อมูล log ที่แตกต่างกันให้อยู่ในรูปแบบเดียวกัน ใส่ลงในช่องมาตรฐานเพื่อให้สามารถบันทึกลงฐานข้อมูลได้ และสามารถนำข้อมูล log มาจัดการได้อย่างชาญฉลาด สามารถสร้างความสัมพันธ์กันระหว่างข้อมูล log ที่แตกต่างกันได้

โซลูชันนี้มาพร้อมกับการสนับสนุนผู้ขายและประเภทของอุปกรณ์ สำหรับยี่ห้ออื่นๆซึ่งยังไม่รองรับในขณะนี้ ผู้ใช้สามารถใช้ฟังก์ชัน GROK เพื่อจัดรูปแบบข้อมูลได้

ต่อไปนี้คือผู้ให้บริการที่รองรับการจัดรูปแบบข้อมูล log ได้ทันที

activemq	apache	auditd	aws	awsfargate	azure	barracuda	bluecoat
cef	checkpoint	cisco	citrix	coredns	crowdstrike	cyberark	cyberarkpas
cylance	elasticsearch	envoyproxy	f5	fortinet	gcp	google_workspace	googlecloud
gsuite	haproxy	ibmmq	icinga	iis	imperva	infoblox	iptables
juniper	kafka	logstash	microsoft	misp	mongodb	mssql	mysql
mysqlenterprise	nats	netscout	nginx	o365	okta	oracle	osquery
panw	pensando	postgresql	proofpoint	rabbitmq	radware	redis	santa
snort	snyk	sonicwall	sophos	squid	suricata	symantec	system
threatintel	tomcat	traefik	zeek	zookeeper	zoom	zscaler	

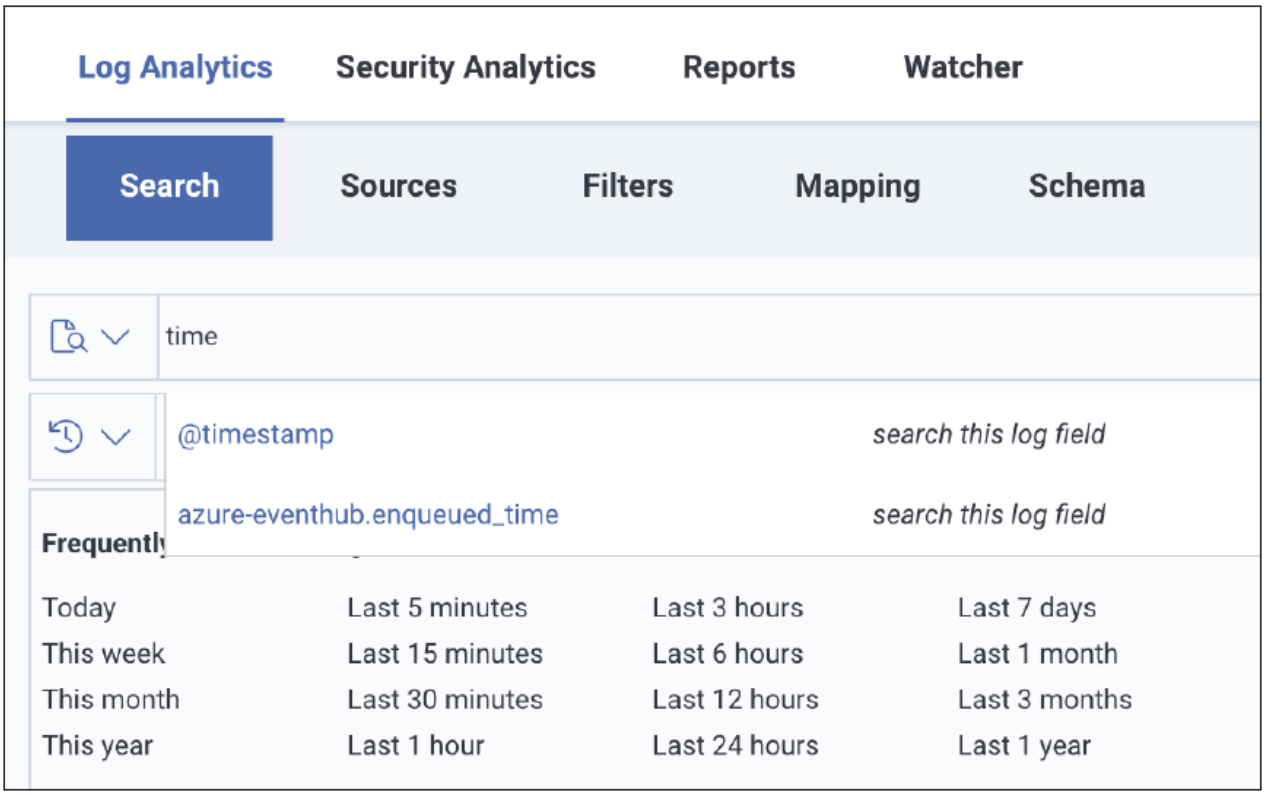
- Mapping to the Elastic Common Schema (ECS)

NetGain ใช้ Elasticsearch เป็นฐานข้อมูลพื้นฐาน และ Filebeat เป็นเครื่องมือหลักในการรวบรวมและจัดรูปแบบข้อมูล log, Filebeat สร้างขึ้นโดยชุมชนผู้ใช้งานเพื่อรองรับอุปกรณ์ล่าสุด โดยจัดรูปแบบข้อมูล log ให้เป็นไปตามมาตรฐาน Elastic Common Schema

- Intelligent search, query and correlation

โมดูลนี้มาพร้อมกับความสามารถในการค้นหาอัจฉริยะที่ให้คำแนะนำในการค้นหา ในขณะที่คุณพิมพ์ การสืบค้นจะทำได้อย่างรวดเร็ว แม้กับชุดข้อมูลขนาดใหญ่ การค้นหายังสามารถดำเนินการได้โดยการเงื่อนไขความสัมพันธ์ของข้อมูล และผลลัพธ์จะแสดงบนหน้าจอได้อย่างเหมาะสม และสามารถนำออกเป็นรูปแบบรายงานได้

GUI ยังอนุญาตให้ผู้ใช้เลือกและช่วงเวลาในการค้นหาได้ตามต้องการ



Security Analytics

Security Analytics ได้รับการออกแบบมาเพื่อวิเคราะห์ภัยคุกคาม จากการเชื่อมโยงข้อมูลระหว่างข้อมูลเหตุการณ์ log ต่างๆโดยอัตโนมัติ จากแหล่งที่มาที่หลากหลาย ข้อมูลเหตุการณ์, ปริมาณการใช้เครือข่าย, โฟลว์ และการตรวจสอบผู้ใช้, กิจกรรมการเข้าสู่ระบบ เพื่อตรวจหาเหตุการณ์ที่อาจเป็นภัยคุกคามที่รู้จักหรือไม่รู้จัก การวิเคราะห์ตรวจหาเหตุการณ์ที่อาจเป็นภัยคุกคามความปลอดภัยนี้อยู่บนพื้นฐานข้อมูลของ Log Analytics

หลังจากรวบรวมข้อมูล log และจัดรูปแบบข้อมูลเป็นไฟล์ส่วนกลางแล้ว ข้อมูลจะถูกเทียบกับกฎการตรวจจับภัยคุกคามอัตโนมัติที่สร้างไว้ล่วงหน้าหลายร้อยรายการ ซึ่งรวมถึง security use cases และอัลกอริทึมการตรวจจับความผิดปกติ และนโยบายความสัมพันธ์ตามเวลาจริง ซึ่งสามารถระบุภัยคุกคามที่รู้จักและที่อาจเป็นไปได้ ได้อย่างรวดเร็ว และการแจ้งเตือน ออกรายงานตามมาตรฐานต่างที่รองรับ

- Threat rules

โซลูชันนี้มาพร้อมกับกฎภัยคุกคามเกือบ 700 ข้อ กฎเหล่านี้เป็นไปตาม MITER ATT&CK framework ซึ่งเป็นหน่วยงานอุตสาหกรรมที่บันทึกการโจมตีที่เป็นที่รู้จักทั่วโลก กฎใหม่จะได้รับการอัปเดตอย่างต่อเนื่องโดย NetGain และผู้ใช้อาจสร้างกฎการคุกคามโดยใช้ query, python script, หรือ Advance Intelligence Workflow ที่เป็นนวัตกรรมใหม่สำหรับลดการ coding ให้น้อยที่สุด

ต่อไปนี้คือหมวดหมู่ของกฎภัยคุกคามที่พร้อมใช้งานทันที:

APM	AWS	Active Directory	Application	Asset Visibility	Azure
Cloud	Collection	Command and Control	Configuration Audit	Credential Access	Data Protection
Defense Evasion	Endpoint Security	Execution	GCP	Google Workspace	Host
Identity	Identity and Access	Impact	Initial Access	Lateral Movement	Linux
Log Auditing	MacOS	Microsoft 365	Network	Okta	Persistence
Post-Execution	Privilege Escalation	Windows	Zoom	cyberarkpas	

- Integration to third-party threat intelligence

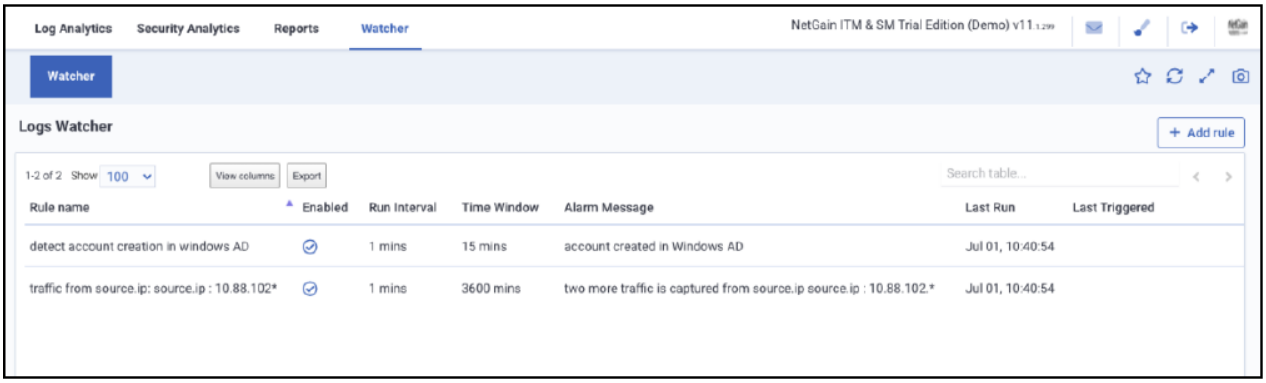
โซลูชันสามารถรวมเข้ากับชุดข้อมูลข่าวกรองภัยคุกคามภายนอกจากแหล่งที่เชื่อถือได้ (external threat intelligence) ผู้ใช้สามารถเพิ่มแหล่งข้อมูลได้ตามต้องการ ตัวอย่างของชุดข้อมูลข่าวกรองภัยคุกคามดังกล่าว ได้แก่ บัญชีดำสำหรับ IP addresses, Domain names หรือข้อมูลอื่นๆที่เป็นข้อมูลจากการถูกบุกรุก

- Intelligent search, query and correlation

สำหรับการวิเคราะห์ความปลอดภัย เมื่อระบบตรวจพบภัยคุกคาม ผู้ใช้จะต้องสามารถตรวจสอบภัยคุกคามได้อย่างรวดเร็วและแม่นยำ ฟังก์ชันการค้นหาที่ทรงพลังจะช่วยให้ทำงานค้นหาได้อย่างรวดเร็วมีประสิทธิภาพแม้กับชุดข้อมูลขนาดใหญ่และเงื่อนไขความสัมพันธ์ของข้อมูล ผลลัพธ์จะแสดงบนหน้าจอได้อย่างเหมาะสม และสามารถนำออกเป็นรูปแบบรายงานได้

Watcher

คุณลักษณะ Watcher ช่วยให้ผู้ใช้สามารถตั้งค่า query based ได้ตาม key words ที่สำคัญ และระบบจะสร้างการแจ้งเตือนไปยังเจ้าหน้าที่ปฏิบัติงานเมื่อมีการพบข้อมูลที่ตรงกับ key words



Report

มีรายงานมาตรฐานหลายร้อยรายการที่ได้กำหนดค่าไว้ ผู้ใช้สามารถรับรายงานได้ตลอดเวลาตามที่ต้องการ และรายงานการปฏิบัติตามข้อกำหนด (standard compliance) เช่น HIPAA ก็ได้จัดเตรียมพร้อมใช้งานทันที และผู้ใช้ก็สามารถสร้างรายงานเฉพาะตามที่ต้องการได้เช่นกัน

CCPA	COCO	CYBER ESSENTIALS	FERPA	FISMA
GDPR	GLBA	GPG	HIPAA	ISLP
ISO 27001 2013	NERC	NIST	NRC	PCI DSS
PDPA	SOX			

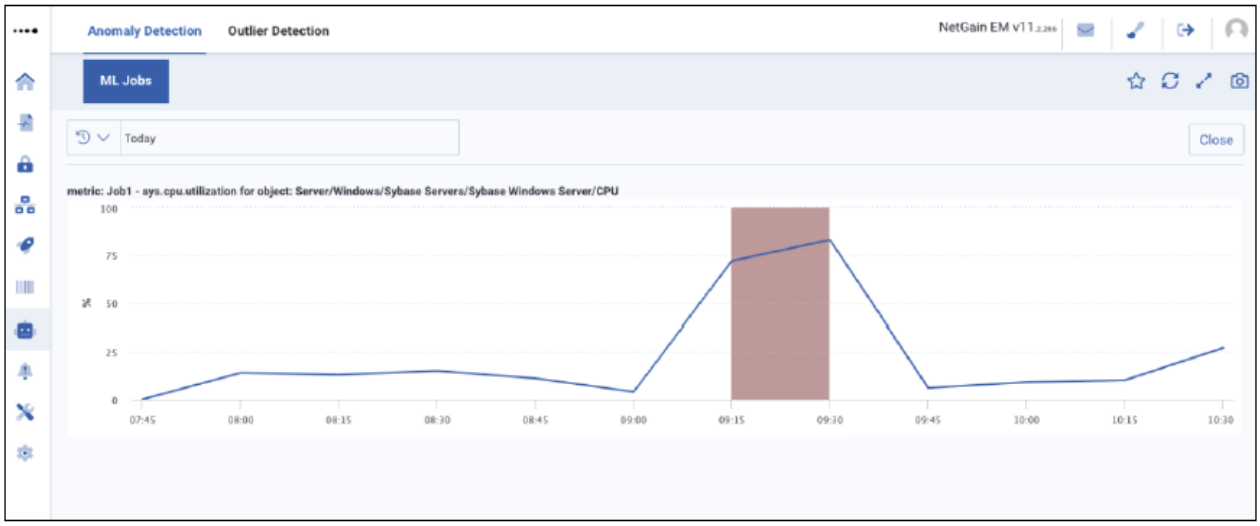
AI Ops

การดำเนินการที่ได้รับความช่วยเหลือจากปัญญาประดิษฐ์ (AI Ops) เป็นโมดูลแยกต่างหากที่ใช้บันทึกที่นำเข้าเพื่อทำหน้าที่ต่อไปนี้:

- Anomaly detection

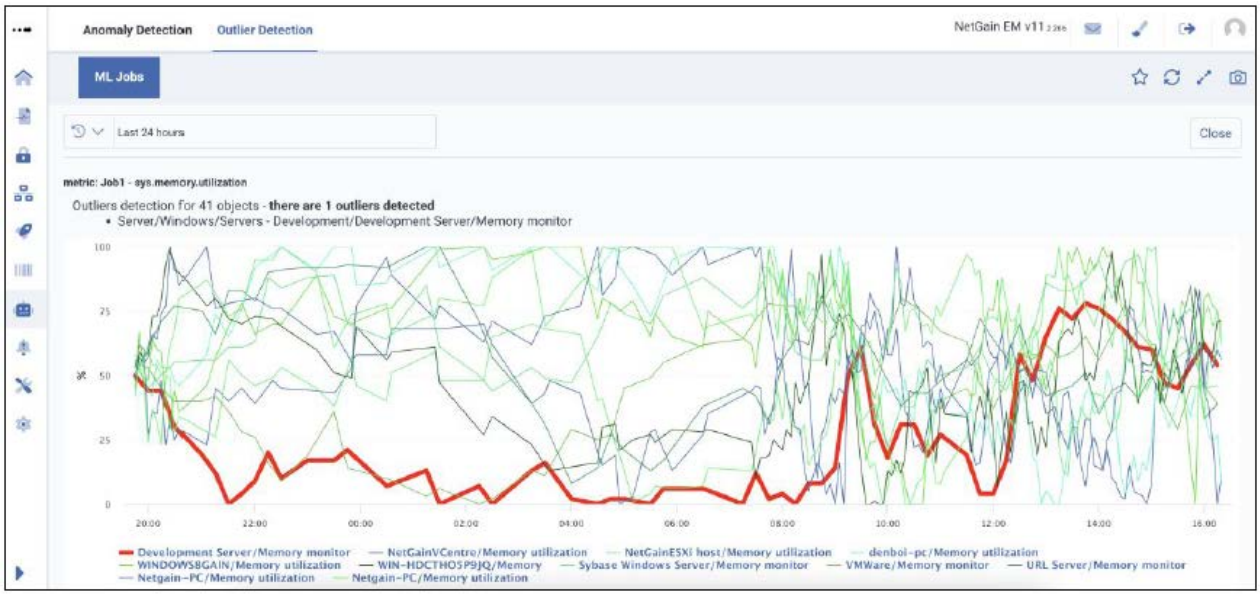
การตรวจจับความผิดปกติ คือการระบุลักษณะการทำงานของส่วนประกอบไอที ที่เบี่ยงเบนไปจากลักษณะการทำงานปกติ ตัวอย่างจะเป็น IP address ต้นทางซึ่งส่งทราฟฟิกไปยังเซิร์ฟเวอร์ เฉพาะระหว่างเวลาชั่วโมงที่ทำงานเท่านั้น อย่างไรก็ตาม หากเริ่มส่งทราฟฟิกไปยังเซิร์ฟเวอร์เดียวกันตอนเที่ยงคืน ถือว่าผิดปกติ โดยการใช้ข้อมูลในอดีต AI จะกำหนดพฤติกรรมพื้นฐานและระบุพฤติกรรมที่เบี่ยงเบนจากพื้นฐานพฤติกรรมที่เกิดขึ้น และฝ่ายไอทีสามารถปรับตั้งค่าความไวของการตรวจจับของ AI ได้

ด้วยการตรวจจับความผิดปกติ เจ้าหน้าที่ฝ่ายไอทีไม่จำเป็นต้องตั้งค่าเกณฑ์คงที่ (static thresholds) แต่พึ่งพา AI เพื่อค้นหาเกณฑ์โดยอัตโนมัติ จากนั้นจึงแจ้งเตือนทีมปฏิบัติการเมื่อเกิดความผิดปกติขึ้น

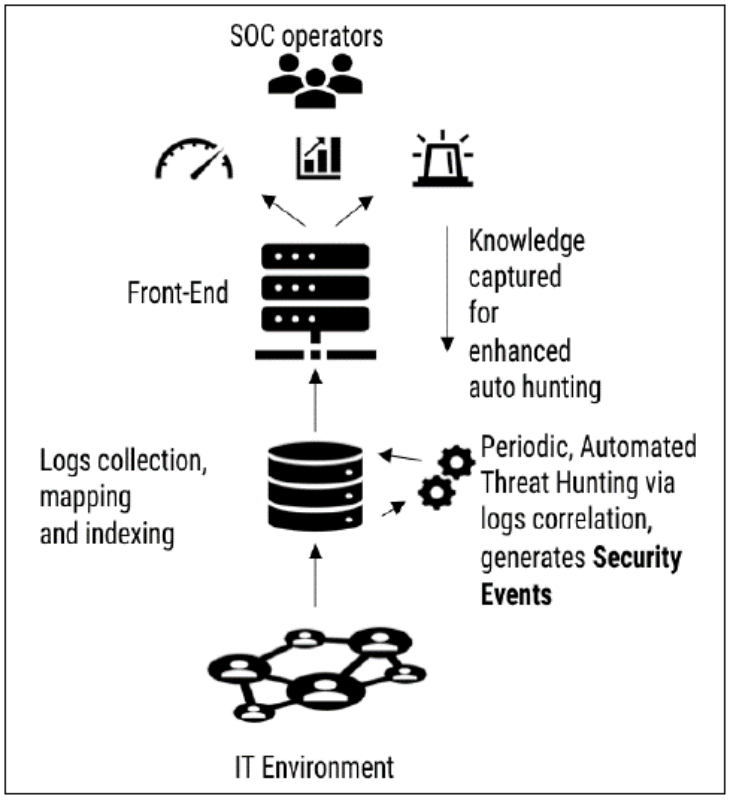


- Outlier detection

ค่าผิดปกติคือองค์ประกอบด้านไอที ที่เบี่ยงเบนอย่างมากจากบรรทัดฐาน หรือค่าเฉลี่ยที่กำหนดของชุดข้อมูล ตัวอย่างเช่น หากเซิร์ฟเวอร์ 20 ชุดกำลังส่ง log ไปยังระบบทั้งหมด และเซิร์ฟเวอร์หนึ่งกำลังส่ง log มากกว่าเซิร์ฟเวอร์อื่น ๆ จะถือว่าเซิร์ฟเวอร์นี้ผิดปกติ AI ใช้เพื่อระบุค่าผิดปกติในชุดข้อมูลที่กำหนด ฝ่ายไอทีสามารถปรับตั้งค่าความไวของการตรวจจับของ AI ได้



How It Works



Log จะถูกรวบรวมและนำเข้าไปยัง NetGain แพลตฟอร์ม log จะมาจากไอทีที่หลากหลาย รวมถึงอุปกรณ์รักษาความปลอดภัย เซิร์ฟเวอร์ และอุปกรณ์เครือข่าย

ข้อมูล log ได้รับการทำให้เป็นมาตรฐานโดยใช้ Elastic Common Schema ซึ่งช่วยให้ข้อมูลจากหลายแหล่งที่มาต่างๆ สามารถเชื่องโยงใช้ในการวิเคราะห์

ผู้ใช้สามารถเริ่มค้นหาได้ง่ายจากการเชื่อมโยงอย่างชาญฉลาดผ่านอินเทอร์เฟซการสืบค้น

สำหรับการวิเคราะห์ความปลอดภัย log จะทำงานค้นหาตามกฎภัยคุกคามโดยอัตโนมัติ และภัยคุกคามใด ๆ ที่ระบุได้รับการแจ้งเตือนไปยังทีมปฏิบัติการไอที

Deploying NetGain Security Analytics

NetGain Security Analytics สามารถนำไปใช้ในเซิร์ฟเวอร์เครื่องเดียวหรือกระจายผ่าน VM หลายเครื่อง appliances หรือ cloud instances สถาปัตยกรรมที่มีความยืดหยุ่นสูงและปรับขนาดได้ ทำให้เข้ากับทุกขนาดได้อย่างง่ายดาย ตามสภาพแวดล้อมที่มีอยู่ และมีความสามารถเพื่อรองรับการเติบโตและการขยายตัวได้ในอนาคต

NetGain Security Analytics สามารถจัดการอุปกรณ์ในโครงสร้างพื้นฐานด้านไอทีของคุณซึ่งครอบคลุมหลายอุปกรณ์ พื้นที่ทางภูมิศาสตร์ ในระบบคลาวด์ และในเครือข่ายทางกายภาพ/คลาวด์แบบไฮบริด โดยใช้ประโยชน์จาก NetGain Cloud Vista Suite ช่วยให้คุณสามารถตรวจสอบและจัดการภัยคุกคามต่อโครงสร้างพื้นฐานด้านไอทีของคุณจากระยะไกลได้จากทุกที่

System Requirements

ข้อกำหนดสำหรับการใช้งาน NetGain Security Analytics จะขึ้นอยู่กับจำนวนของอุปกรณ์และขนาดของเครือข่ายที่มีการปรับใช้ ต่อไปนี้เป็นการบ่งชี้ถึงข้อกำหนดด้านฮาร์ดแวร์สำหรับสภาพแวดล้อมไอทีที่กำหนด โปรดติดต่อ NetGain เกี่ยวกับข้อกำหนดที่เหมาะสมสำหรับสภาพแวดล้อมของคุณ

Managed Security Analytics environment: Up to 100 devices, consisting of 1-10 firewalls, 10-40 switches/routers, and 20-40 Windows or Linux servers/containers **Data Retention period:** 6 months	
Hard disk	2TB
CPU	Quad Core
RAM	16GB
Operating System	CentOS 7, RHEL 8 or equivalent
Browsers Supported	Firefox, Google Chrome, Safari, Microsoft Edge.

About NetGain Systems

NetGain Systems ก่อตั้งขึ้นในปี 2545 เป็นผู้บุกเบิกในธุรกิจการตรวจสอบด้านไอที และยังคงพัฒนาธุรกิจอย่างต่อเนื่อง เพื่อพัฒนาการตรวจสอบด้านไอทีไปสู่ความสามารถในการสังเกตการณ์ด้านไอที บริษัทได้จัดตั้งทีมงานท้องถิ่นทั่วภูมิภาคเอเชียแปซิฟิก รวมถึงออสเตรเลีย จีน สิงคโปร์ และไทย

โดยไม่คำนึงถึงสถานที่ตั้ง ประเภท ขนาด หรือความซับซ้อน โซลูชันของเราช่วยให้ลูกค้าของเรามีอำนาจในการสังเกตการณ์โครงสร้างพื้นฐานด้านไอที บริการ แอปพลิเคชัน และอุปกรณ์ได้อย่างง่ายดาย จากแดชบอร์ดการจัดการเดียว เพื่อให้บรรลุความเป็นเลิศในการดำเนินงานโดยลดความซับซ้อนลงและรับข้อมูลเชิงลึกที่เป็นประโยชน์ เพื่อปรับปรุงผลลัพธ์ทางธุรกิจ

ด้วยการทำความเข้าใจว่าสภาพแวดล้อมด้านไอทีขององค์กรแต่ละแห่งมีความแตกต่างกัน โซลูชันแบบไดนามิกของ NetGain ได้รับการออกแบบมาให้ปรับเปลี่ยนได้อย่างเหมาะสม กับความต้องการเฉพาะของสภาพแวดล้อมการดำเนินงานของคุณ และพัฒนาไปพร้อมกับองค์กรที่กำลังเติบโตของคุณ