CALA SECURITY

Correlyze Advance Log Analytics

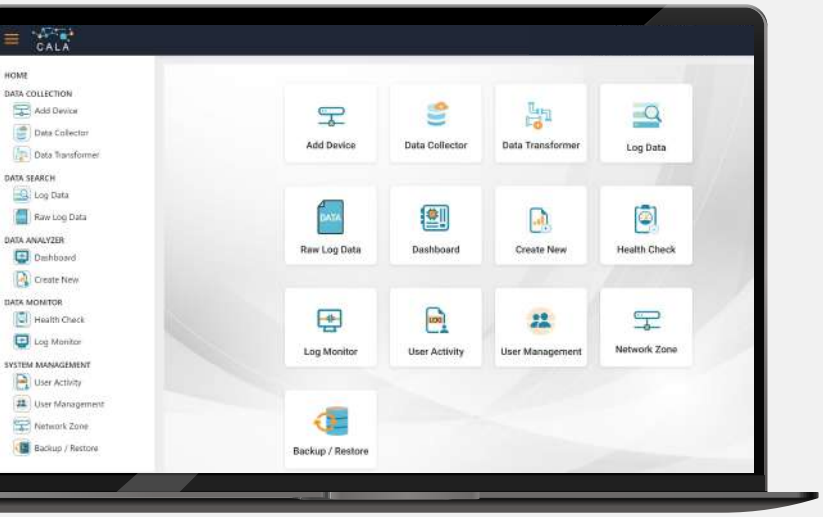
CALA Security

ระบบรวบรวม จัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (Log File) ที่เกิดขึ้นบนอุปกรณ์เครือข่ายระบบคอมพิวเตอร์ ระบบปฏิบัติการ เครื่องแม่ข่าย หรือระบบงานคอมพิวเตอร์ต่าง ๆ ภายในองค์กร เช่น Network Devices, Firewall, Switch, Operating System, Database System ให้สอดคล้องเป็นไปตาม พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 สามารถจัดเก็บข้อมูลได้ไม่น้อยกว่า 90 วัน พร้อมด้วยความสามารถในการสืบค้น (Search) คัดกรอง (Filter) วิเคราะห์ (Analytic) แจ้งเตือน (Alert) และรายงานสรุปผล (Dashboard) เพื่อช่วยในการติดตาม ตรวจสอบ แก้ไขและป้องกันความเสียหายที่จะเกิดขึ้น

CORRELYZE ADVANCE LOG ANALYTICS

- Beyond log management
- Scalable architecture
- Log data visibility & Log analytics
- Flexible dashboard
- Proactive protection
- Easy & rapid investigation
- Comply computer Act.
- Simple & affordable

PROTECT YOUR ORGANIZATION FROM CYBERATTACKS

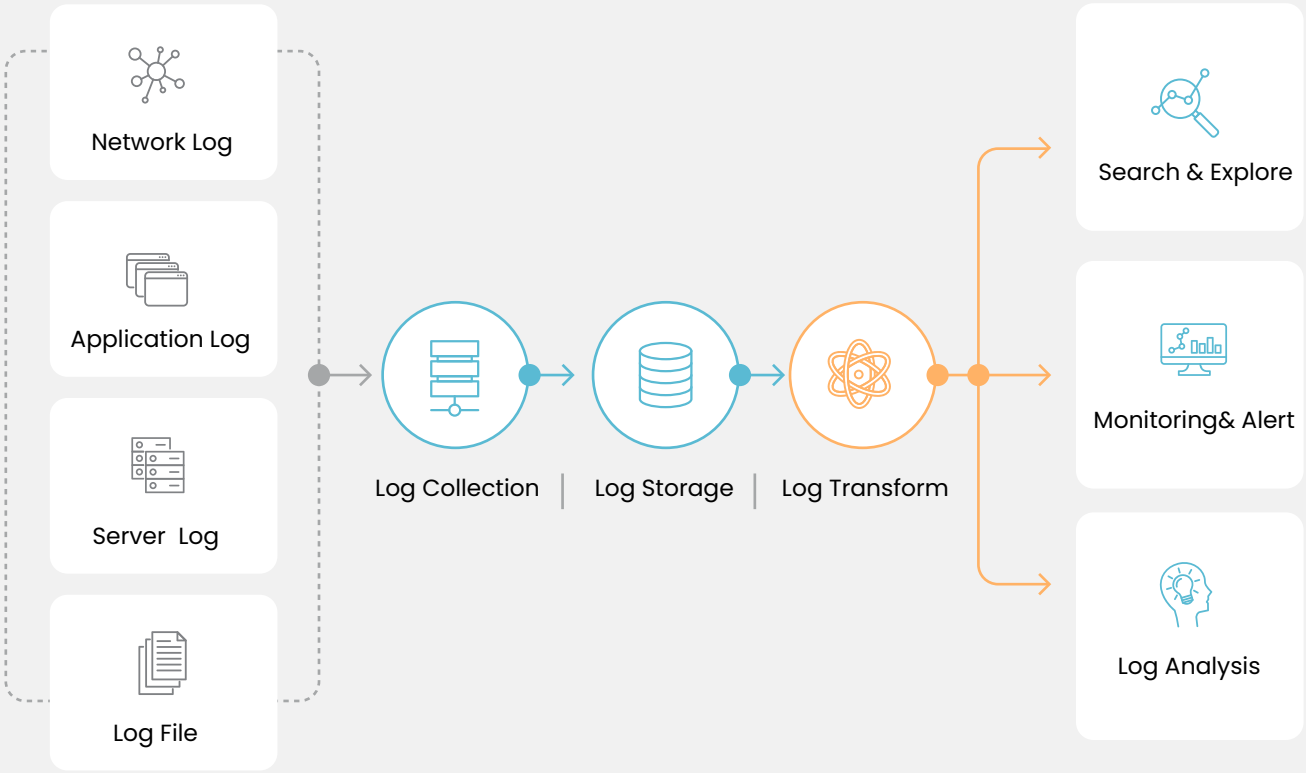


ภารกิจสำคัญที่เป็นความท้าทายของทุกองค์กรในยุคดิจิทัลทรานส์ฟอร์มเมชัน (Digital Transformation) คงหนีไม่พ้นเรื่องของการดูแลด้านความปลอดภัยของระบบไซเบอร์ แม้จะพยายามป้องกันอย่างเต็มกำลัง การละเมิด บุกรุก คุกคามยังคงมีแนวโน้มเกิดขึ้นอย่างต่อเนื่อง ไม่ว่าจะเป็นเหตุการณ์ขโมยข้อมูลโดยบุคคลภายนอก และนำข้อมูลส่วนบุคคลไปใช้ในทางที่ผิด ภัยคุกคามเหล่านี้ส่งผลกระทบอย่างยิ่งต่อการดำเนินธุรกิจ ความเชื่อมั่นและชื่อเสียงขององค์กร

ดังนั้น Log Management และ Log Analytics จึงเป็นเทคโนโลยีด้านความปลอดภัยที่ทุกองค์กรต้องใช้เพื่อรับมือกับภัยคุกคามที่มีความซับซ้อนสูงภายในระบบสารสนเทศที่ต้องใช้อุปกรณ์จำนวนมากและหลากหลาย

CALA Security

Overview



HOW CALA SECURITY HELPS ORGANIZATION?

Data Collection

รวบรวม จัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (Log File) ที่เกิดจากอุปกรณ์เครือข่ายระบบคอมพิวเตอร์, ระบบปฏิบัติการ, เครื่องแม่ข่าย หรือระบบงานคอมพิวเตอร์ต่าง ๆ ภายในองค์กร ในรูปแบบ Machine Data เช่น Log File, Flat Files ผ่าน Protocol Syslog , Non-Syslog, Syslog Agent เพื่อการวิเคราะห์และรองรับการส่งข้อมูล Log เข้ามาจัดเก็บผ่าน FTP Protocol

Data Transform

แปลงและจัดเก็บข้อมูล Log ให้อยู่ในรูปแบบที่ง่ายต่อความเข้าใจและการนำไปใช้งาน (Business Log) แยกจากข้อมูล log ต้นทาง (Original Log) ที่จัดเก็บโดยไม่มีการเปลี่ยนแปลงข้อมูล

Data Search

สืบค้น (Search) เรียกดูข้อมูลได้อย่างง่ายและรวดเร็ว ด้วย Search Engine ที่มีประสิทธิภาพสูง สามารถกำหนดเงื่อนไขเพื่อคัดกรอง (Filter) ข้อมูลในเชิงลึกตามที่ต้องการ เช่น Source/Destination IP, Source/Destination Port ,IP Address, Date & Time, Specify Conditions, Keyword รวมถึงการค้นหาแบบ Full-text Search โดยสามารถสืบค้น เรียกดูข้อมูลทั้งแบบย้อนหลัง และ แบบ Real-time

Data Integrity

มีระบบยืนยันความสมบูรณ์ถูกต้อง และเที่ยงตรงของข้อมูล Log ที่จัดเก็บในระบบตามมาตรฐาน MD5 ภายใต้การจัดเก็บแบบ Object Storage

Log Retention Period

ระยะเวลาการเก็บรักษา (Retention Period) ข้อมูล Log ไม่น้อยกว่า 90 วันนับตั้งแต่วันที่ข้อมูลเข้าสู่ระบบ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 26

Data Monitoring

รายงานและแผงควบคุม (Report & Dashboard Monitoring) สำหรับติดตามข้อมูล เหตุการณ์ผิดปกติ เพื่อวิเคราะห์และตรวจสอบข้อมูลเชิงลึก (Drill Down) ได้ เช่น ปริมาณ Traffic Log ที่ส่งเข้ามาจัดเก็บในระบบ แยกตามอุปกรณ์ ตามช่วงเวลา , Top 10 Traffic Log ที่ส่งเข้ามาจัดเก็บในระบบ เป็นต้น

Data Analyzer and Chart Visualization

ผู้ใช้สามารถสร้างและปรับเปลี่ยนรายงานและแผงควบคุม (Create Report & Dashboard) ในรูปแบบ Chart ต่าง ๆ เช่น Pie Chart, Line Chart, Bar Chart, Area Chart, Map Graph, Table เป็นต้น

System Alert

ระบบแจ้งเตือน (Alert) เมื่อตรวจพบข้อมูล เหตุการณ์ หรือความผิดปกติ ไปยังผู้ดูแลระบบหรือปลายทาง ผ่าน User Interface ของระบบ, Line Notification, E-mail เพื่อตรวจสอบ แก้ไข ก่อนเกิดความเสียหาย โดยสามารถตั้งค่า รูปแบบ, กฎ, เงื่อนไข ในการแจ้งเตือนได้

Log Forwarding

รองรับการส่งต่อข้อมูล Log แบบ Real-time ในลักษณะ Output UDP ไปภายนอกระบบ โดยไม่มีการเปลี่ยนแปลงข้อมูลต้นทาง

System Monitoring

ระบบตรวจสอบการทำงานของโมดูลต่าง ๆ ในลักษณะ Real-time และแจ้งเตือนความผิดปกติ ของ CPU Utilization, Memory Utilization, Disk Utilization ผ่าน System Alert

Log Monitoring

ระบบตรวจสอบสถานะการรับข้อมูล เมื่อไม่มีข้อมูล Log ส่งมาจากอุปกรณ์นานเกินกว่าเวลาที่กำหนด และแจ้งเตือนไปยังผู้ดูแลระบบผ่าน System Alert

User Management

มีระบบบริหารจัดการผู้ใช้งาน สามารถกำหนดผู้ใช้งาน กลุ่มผู้ใช้งาน บทบาทและสิทธิการใช้งานระบบของผู้ใช้งานได้

System Architecture

- ระบบออกแบบบนเทคโนโลยีโครงสร้างพื้นฐานที่เป็น Open Platform ในลักษณะ Container รองรับการ Scale-Out หรือ Horizontal กรณีมีปริมาณข้อมูลมากขึ้นในอนาคต รวมถึงระบบทำงานอยู่บนเทคโนโลยี จัดเก็บและจัดการข้อมูลในลักษณะ Object Storage และมีฐานข้อมูลที่ไม่เป็น proprietary รองรับการเรียกใช้งาน/ค้นหาข้อมูลด้วยภาษา SQL มาตรฐาน ผ่าน ODBC, JDBC, Web Service เป็นต้น

- ระบบเป็น Web-based application ทำงานผ่าน Web Browser บนเครื่องคอมพิวเตอร์ (Desktop), Smart Phone, Tablet โดยใช้เทคโนโลยี Responsive รองรับการแสดงผลที่แตกต่างกันในแต่ละอุปกรณ์

FEATURE AND SPECIFICATION

Feature	Specification
System Architecture	Container, Responsive Web-based application, and Search Engine
Data Collection	Syslog, Syslog Agent, UPD Protocol, TCP Protocol
Data Transform	Data Transform for Enhanced Search Engine
Data Search Technology	Search Engine
Data Integrity	MD5 object storage
Log Retention Period	Comply to the Computer Act B.E. 2017 by storing data for not less than 90 days.
Data Monitoring	Dashboard Monitoring for Tracking Traffic Log by Device
Data Analyzer and Chart Visualization	User Dashboard Customization
System Alert	Alert for User Interface, Line Notification, E-mail
Log Forwarding	Can Forward Log to another Device
System Monitoring	Monitoring System Resource for CPU Utilization, Memory Utilization, Disk Utilization
Log Monitoring	Check the status of receiving log data from the device
User Management	Manage User, Group, Role

WHY CALA SECURITY BY CDGS?

Professional System Integrator in Thai-land

System Integrator รายแรกของประเทศไทย

Experienced & Specialized Tech Personnel

ทีมงานที่มีประสบการณ์และความเชี่ยวชาญด้านเทคโนโลยี ครอบคลุมทุกส่วนงาน

Total Project Management Services

บริการบริหารโครงการแบบครบวงจร ด้วยทีมงานมืออาชีพ

Over 50 Years of Services

ส่งมอบผลงานคุณภาพ ที่ลูกค้าพึงพอใจมายาวนานกว่า 50 ปี

Trusted by 100+ public sector and state-enterprises

ลูกค้าทั้งภาครัฐและรัฐวิสาหกิจกว่า 100 หน่วยงาน ไว้วางใจในคุณภาพการบริการ

CALA SECURITY
Correlyze Advance Log Analytics

บริษัท ซีดีจี ซิสเต็มส์ จำกัด
202 อาคารซีดีจีเฮ้าส์ ถนนนางลิ้นจี่ แขวงช่องนนทรี เขตยานนาวา กรุงเทพมหานคร 10120
โทรศัพท์ : 02-678-0978 | โทรสาร : 02-678-0321 | www.cdgs.co.th