ระบบตรวจสอบการใช้งานระบบฐานข้อมูลในเครือข่าย (Database Firewall) พร้อมติดตั้ง
แขวงคลองเตยเหนือ เขตวัฒนา กรุงเทพมหานคร จำนวน 1 ระบบ
สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ

รายละเอียดคุณลักษณะเฉพาะ

1. เป็น Virtual Appliance ที่ถูกออกแบบมาสำหรับทำหน้าที่ด้าน Database Security โดยเฉพาะ
2. สามารถเก็บข้อมูลการใช้งาน (Database Audit หรือ Database Activity Monitor) รวมถึง Response audit data และป้องกันความปลอดภัยให้กับฐานข้อมูล (Database Firewall) ได้
3. สามารถรองรับการติดตั้งบน VMware ESX/ESXi ได้เป็นอย่างน้อย โดยจะต้องเสนอเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่มีประสิทธิภาพเพียงพอต่อระบบงานด้าน Database Security
4. สามารถในการทำ Database Security ได้ไม่น้อยกว่า 6,000 TPS
5. สามารถติดตั้งแบบ Transparent bridge (Inline), sniffing และ Agent ได้เป็นอย่างน้อย
6. มี Agent ในการช่วยตรวจสอบและวิเคราะห์การใช้งานที่ Database Server ได้ ไม่น้อยกว่า 25 Database Server
7. รองรับการทำงานกับฐานข้อมูลที่ติดตั้งอยู่บนระบบปฏิบัติการ Windows, HP-UX, Red Hat, Oracle Enterprise Linux (OEL), Solaris, SUSE, Ubuntu และ AIX ได้
8. สามารถรองรับการ Monitor ระบบจัดการฐานข้อมูลต่อไปนี้ ได้แก่ MSSQL, MySQL, MariaDB, Oracle, Informix, DB2, Sybase, PostgreSQL, Greenplum, Netezza และ SAP HANA ได้เป็นอย่างน้อย
9. สามารถกำหนด Audit Policy และ Security Policy ขึ้นเองได้โดยมีชุดเกณฑ์เงื่อนไข (Match Criteria) สำหรับการสร้าง policy โดยเฉพาะ
10. สามารถทำ Database Activity Monitoring, โดยสามารถแสดงข้อมูลของผู้ที่เข้ามาใช้บริการ เช่น data records, Shared Database User, Sensitive Query, Top Queries, Data Modification, DCL Commands, DDL Commands, และ SQL Errors ได้
11. สามารถทำการตรวจจับการโจมตีระบบจัดการฐานข้อมูลได้ โดยมีระบบการตรวจจับการโจมตีเช่น DB Protocol Validation และDB Service Correlated Validation, Signature พร้อมการ update ระบบการตรวจจับการโจมตีได้โดยอัตโนมัติ

12. มีระบบเรียนรู้พฤติกรรมการใช้งานของ Database User เช่น Source IP Address, OS Hostname, Source Application, Database, Table, และ Query ได้เป็นอย่างน้อย และสามารถนำข้อมูลจากระบบเรียนรู้พฤติกรรม database user มาทำ security policy ได้
13. สามารถทำ Vulnerability Assessment อย่างน้อย 1,500 pre-defined vulnerability tests ทั้งในส่วนของ Operating system and database vulnerabilities และ Configuration ได้โดยมี assessment policies และระบบจัดการฐานข้อมูลเช่น Oracle, MSSQL, Informix, Sybase, DB2, MySQL, CIS, PCI-DSS, HIPPA, DISA (STIG) และ FISMA ได้
14. สามารถทำ Data Classification สำหรับการค้นหาข้อมูล Sensitive Data ใน Database เช่น ชื่อ, ที่อยู่, เบอร์โทรศัพท์ และหมายเลขประจำตัว ได้ และสามารถกำหนดรูปแบบการค้นหาข้อมูลเองได้ และสามารถกำหนด Scheduling ในการทำ Data Classification ได้
15. สามารถป้องกันการโจมตีแบบ no latency และ holds events ได้
16. สามารถส่งข้อมูล audit archive โดยมีการเข้ารหัสไปเก็บยังระบบภายนอกแบบ FTP, SCP ได้ และสามารถนำข้อมูล Archived data ที่ส่งออกไปยัง external storage นำกลับมาแสดงผลได้
17. สามารถส่งข้อมูล audit logs ไปยัง SIEM platforms ในรูปแบบ CEF และ json ได้
18. มีระบบบริหารจัดการแบบรวมศูนย์ (Centralize Management) สำหรับบริหารจัดการด้านการตั้งค่าระบบ, การตรวจสอบ และการทำรายงาน สำหรับ Database Security โดยเฉพาะในรูปแบบ Virtual Appliance
19. ผู้ยื่นข้อเสนอจะต้องมีหนังสือแสดงการเป็นผู้มีสิทธิจำหน่ายผลิตภัณฑ์ที่เสนอจากผู้ผลิตหรือจากสาขาของผู้ผลิตในประเทศไทย
20. ติดตั้งที่ห้องคอมพิวเตอร์กลาง สำนักคอมพิวเตอร์ ชั้น 2 อาคารคณะศิลปกรรมศาสตร์
21. รับประกันไม่น้อยกว่า 3 ปีแบบ Onsite Services
