HỌC VIỆN QUÂN Y
BỆNH VIỆN QUÂN Y 103

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 24 tháng 10 năm 2025

YÊU CẦU BÁO GIÁ
Về việc thuê dịch vụ giám sát an toàn thông tin mạng 24/7

Kính gửi: Quý đơn vị cung cấp phần mềm

Trước hết Bệnh viện Quân y 103 xin trân trọng cảm ơn sự phối hợp, hợp tác của các đơn vị, nhà cung cấp với Bệnh viện trong suốt thời gian qua.

Hiện nay, Bệnh viện Quân y 103 đang có nhu cầu thuê dịch vụ giám sát an toàn thông tin mạng 24/7. Để có cơ sở lập dự toán, kế hoạch thuê, Bệnh viện kính mời các đơn vị có khả năng cung cấp dịch vụ giám sát an toàn thông tin mạng 24/7 gửi báo giá về Bệnh viện Quân y 103 theo các thông tin sau:

1. Danh mục, số lượng, yêu cầu về phần mềm

- Số lượng: 01 dịch vụ.

- Thời gian thuê: 12 tháng.

- Thông số kỹ thuật chi tiết: Tại phụ lục kèm theo.

2. Hồ sơ báo giá:

2.1. Nội dung báo giá:

- Tên sản phẩm, thông số kỹ thuật, đơn giá (đã bao gồm thuế, chi phí cài đặt, hướng dẫn sử dụng tại Bệnh viện Quân y 103, số 261 đường Phùng Hưng, phường Hà Đông, TP Hà Nội).

- Bảng giá kèm thông tin mô tả chi tiết phần mềm.

2.2. Hồ sơ năng lực của nhà thầu:

- Hồ sơ năng lực, Hợp đồng tương tự (nếu có).

- Giấy đăng ký kinh doanh.

3. Thời gian nhận báo giá: Trong vòng 5 ngày, kể từ ngày đăng tải yêu cầu báo giá.

4. Phương thức báo giá: Báo giá gửi trực tiếp hoặc gửi qua đường công văn, bưu điện.

5. Địa điểm nhận báo giá: Phòng Kế hoạch - Tổng hợp, Bệnh viện Quân y 103.

Địa chỉ: số 261 đường Phùng Hưng, phường Hà Đông, Hà Nội.

Số điện thoại: Liên hệ 038.667.7668

Xin trân trọng cảm ơn sự hợp tác của Quý đơn vị./.

Nơi nhận:
- Như trên;
- Lưu: VT, KHTH, M03.

GIÁM ĐỐC

HỌC VIỆN QUÂN Y
BỆNH VIỆN QUÂN Y 103

Thiếu tướng Lường Công Thức

Phụ lục

THÔNG SỐ KỸ THUẬT DỊCH VỤ
GIÁM SÁT AN TOÀN THÔNG TIN MẠNG

(Kèm theo Yêu cầu báo giá ngày 24/10/2025 của Bệnh viện Quân y 103)

TT	Danh mục	Thông số kỹ thuật	Số lượng	Ghi chú
1	Dịch vụ giám sát An toàn thông tin mạng 24/7	- Số lượng máy chủ: 03 thiết bị. - Hệ thống Trung tâm giám sát ATTT trên nền tảng giám sát toàn diện Open XDR. - Giao diện quản trị riêng biệt để theo dõi giám sát. - Hệ thống thu thập thập log từ các thiết bị mạng, thiết bị bảo mật (SIEM). + Lưu trữ log online 03 tháng. + Phát hiện và cảnh báo sớm các tấn công có chủ đích nhờ giám sát hệ thống một cách toàn diện theo thời gian thực. + Cấu trúc dữ liệu được chuẩn hoá, dễ hiểu và có thể tích hợp đa dạng, linh hoạt với các hệ thống sẵn có khác. - Hệ thống điều phối, tự động hóa và phản ứng an ninh mạng (SOAR). - Xử lý sự cố 24/7; - Giám sát, cảnh báo ATTT 24/7. + Giám sát ATTT Endpoint: Phát hiện thiết bị đầu cuối nhiễm mã độc APT; + Giám sát ATTT lớp mạng: Phát hiện kết nối C&C trong phân vùng mạng có máy chủ cần giám sát; Phát hiện Shellcode/Payload tấn công trong traffic mạng thuộc phân vùng mạng có máy chủ cần giám sát; + Điều tra, xác minh sự kiện: Điều tra, xác minh sự kiện ATTT từ xa. + Gửi cảnh báo đến quản trị viên - Tối ưu ATTT: + Bổ sung rule/usecase phát hiện kỹ thuật tấn công mới + Tối ưu rule/usecase phát sinh nhiều cảnh báo sai - Báo cáo ATTT: + Tình hình vận hành, giám sát theo chuẩn PCI DSS; + Báo cáo xử lý sự cố (nếu có).	01	