UBND TỈNH KON TUM **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do –Hạnh phúc**
Số: 1947/STTTT-HCTH	*Kon Tum, ngày 15 tháng 11 năm 2024*

THƯ MỜI CHÀO GIÁ

Về việc phí dịch vụ Thẩm định giá thuê dịch vụ công nghệ thông tin Hệ thống đảm bảo an toàn thông tin SOC tỉnh Kon Tum, giai đoạn 2024-2026

Kính gửi: Các đơn vị cung ứng dịch vụ Thẩm định giá

Căn cứ Luật Đấu thầu năm 2023; Căn cứ Nghị định số 24/2024/NĐ-CP ngày 27 tháng 02 năm 2024 của Chính phủ Quy định chi tiết một số điều và biện pháp thi hành luật đấu thầu về lựa chọn nhà thầu;

Để có cơ sở xác định giá nhằm tổ chức xây dựng dự toán và kế hoạch lựa chọn nhà thầu theo quy định của nhà nước. Sở Thông tin và Truyền thông Kon Tum kính mời quý đơn vị/Công ty có đầy đủ tư cách pháp nhân, có dầy đủ điều kiện theo quy định của pháp luật tham gia báo giá phí dịch vụ Thẩm định giá thuê dịch vụ công nghệ thông tin Hệ thống đảm bảo an toàn thông tin SOC tỉnh Kon Tum, giai đoạn 2024-2026 *(Có danh mục kèm theo)*.

- Mỗi đơn vị chỉ được gửi 01 báo giá.
- Bên dự chào giá đồng ý cho bên mời chào giá được quyền sử dụng hoặc loại bỏ các bảng báo giá mà không phải thông báo về lý do với đơn vị tham gia chào giá.
- Đề nghị quý công ty/đơn vị gửi bảng chào giá đến chúng tôi bằng văn bảng có đóng dấu của quý công ty/đơn vị trước **17h ngày 18/11/2024** qua địa chỉ: Sở Thông tin và truyền thông Kon Tum, số 112E Bà Triệu, TP Kon tum, tỉnh Kon Tum.

Sở Thông tin và Truyền thông rất mong nhận được sự quan tâm và gửi bảng chào giá của quý công ty/đơn vị ./.

Nơi nhận:
- Như trên;
- Trang TTĐT sở TTTT(đăng tin);
- Lưu: VT, HCTH.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH KON TUM

Trần Văn Thu

Danh mục thuê dịch vụ công nghệ thông tin Hệ thống đảm bảo an toàn thông tin SOC tỉnh Kon Tum, giai đoạn 2024-2026

1. Thuê dịch vụ công nghệ thông tin: Hệ thống đảm bảo an toàn thông tin SOC tỉnh Kon Tum, giai đoạn 2024-2026

TT	Danh mục mua sắm	ĐVT	Số lượng	Thời gian thuê
1	Chi phí thuê Hệ thống đảm bảo an toàn thông tin SOC tỉnh Kon Tum, giai đoạn 2024-2026	Hệ thống	01	36 tháng
2	Chi phí thực hiện giám sát, ứng cứu sự cố an toàn thông tin mạng, bảo vệ hệ thống thông tin	Hệ thống	01	36 tháng

2. Chức năng của hệ thống:

STT	Danh sách chức năng	Ghi chú
A	**SOC Dashboard**	
I	**Quản lý người dùng**	
1	Đăng nhập sử dụng phương thức xác thực đa yếu tố	
2	Quên mật khẩu	
3	Đăng xuất hệ thống	
4	Xem thông tin cá nhân	
5	Quản lý phiên đăng nhập	
II	**Giám sát và thống kê dữ liệu an toàn thông tin**	
6	Giám sát toàn bộ sự kiện an ninh mạng theo thời gian thực (all offense)	
7	Giám sát toàn bộ sự kiện an ninh mạng đang diễn ra theo thời gian thực (open offense)	
8	Giám sát tấn công mạng Brute force	
9	Giám sát tấn công mạng Dos/DDoS	
10	Giám sát tấn công mạng Recon/Scan	
11	Giám sát tấn công Web Exploit	
12	Giám sát Malware trong hệ thống	
13	Giám sát về các cảnh báo System	

14	Giám sát về các cảnh báo Application	
15	Giám sát về các cảnh báo logs Access	
16	Giám sát cảnh báo tấn công mạng Attack Map	
17	Giám sát sự kiện an toàn thông tin theo thời gian thực	
18	Xem thống kê top địa chỉ IP attacker	
19	Xem thống kê top địa chỉ IP bị tấn công	
20	Xem thống kê top 10 loại tấn công	
21	Xem thống kê top 10 IP mã độc	
22	Thay đổi thời gian thống kê sự kiện	
23	Thay đổi thời gian để sự kiện mới nhất được cập nhật	
24	Giám sát và thống kê dữ liệu an toàn thông tin theo Hạ tầng triển khai	
25	Giám sát và thống kê dữ liệu an toàn thông tin theo Hệ thống quản lý	
26	Giám sát và thống kê dữ liệu an toàn thông tin theo Nguồn log	
27	Bảng thống kê Hệ thống giám sát	
28	Xuất dữ liệu Dashboard ra file JSON	
29	Chia sẻ dữ liệu Dashboard	
III	**Quản lý dữ liệu và bảng giám sát (Dashboard)**	
30	Thống kê số lượng sự kiện	
31	Biểu đồ trạng thái xử lý theo sự kiện	
32	Xem thống kê top địa chỉ IP tấn công theo sự kiện	
33	Xem thống kê top địa chỉ IP bị tấn công theo sự kiện	
34	Truy vấn sự kiện an toàn thông tin	
35	Xem thống kê chi tiết sự kiện	
36	Xuất báo cáo thống kê dạng CSV file	
B	**SOC Ticket**	
I	**Quản lý Tickets**	
37	Tạo Tickets	
38	Xem thông tin tất cả sự kiện, sự cố Ticket đang có	
39	Xem thông tin tất cả sự kiện, sự cố Ticket đang mở (open)	
40	Xem thông tin tất cả sự kiện, sự cố Ticket đã hoàn thành (resolve)	
41	Xem thông tin tất cả sự kiện, sự cố Ticket đã đóng (closed)	
42	Xem thông tin tất cả sự kiện, sự cố Ticket của đơn vị	
43	Xem thông tin tất cả sự kiện, sự cố Ticket mức Critical	

44	Xem thông tin tất cả sự kiện, sự cố Ticket mức High	
45	Xem thông tin tất cả sự kiện, sự cố Ticket mức Normal	
46	Xem thông tin tất cả sự kiện, sự cố Ticket báo cáo ngày	
47	Xem thông tin tất cả sự kiện, sự cố Ticket của cá nhân đã tạo	
48	Tìm kiếm Tickets	
49	Xem nội dung Tickets và cập nhật hiện trạng xử lý sự cố	
50	Thay đổi trạng thái phiếu (resolve phiếu sau khi đã xử lý xong sự cố)	
C	**Quản lý và phân tích sự kiện an toàn thông tin - SIEM**	
I	**Quản trị hệ thống**	
I.1	**Quản lý vận hành**	
51	Cho phép thiết lập, thay đổi, áp dụng và hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình tập luật bảo vệ	
52	Cho phép thay đổi thời gian hệ thống	
53	Cho phép thay đổi thời gian duy trì phiên kết nối	
54	Cho phép thiết lập, thay đổi các tham số giới hạn đối với kết nối quản trị từ xa (ví dụ: giới hạn địa chỉ IP, giới hạn số phiên kết nối quản trị từ xa đồng thời,…)	
55	Cho phép đăng xuất tài khoản người dùng có phiên kết nối còn hiệu lực	
56	Cho phép tìm kiếm dữ liệu log bằng từ khóa để xem lại	
57	Cho phép xóa log	
58	Cho phép xem thời gian hệ thống chạy tính từ lần khởi động gần nhất	
I.2	**Quản lý từ xa (VPN)**	
59	Sử dụng giao thức có mã hóa như TLS hoặc tương đương	
60	Tự động đăng xuất tài khoản và hủy bỏ phiên kết nối quản trị từ xa khi hết thời gian duy trì phiên kết nối	
I.3	**Quản lý xác thực và phân quyền**	
61	Hỗ trợ phương thức xác thực bằng tài khoản - mật khẩu, trong đó quản trị viên có thể thiết lập và thay đổi được độ phức tạp của mật khẩu	
62	Hỗ trợ phân nhóm tài khoản tối thiểu theo 02 nhóm là quản trị viên và người dùng thường với những quyền hạn cụ thể đối với từng nhóm	
I.4	**Quản lý báo cáo**	

63	Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo	
64	Cho phép tạo báo cáo mới theo các mẫu báo cáo đã được định nghĩa trước	
65	Cho phép áp dụng các quy tắc tìm kiếm thông tin, dữ liệu log để thêm, lọc, tinh chỉnh nội dung cho báo cáo	
66	Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 02 trong các định dạng sau: WORD, EXCEL, PDF, HTML, XML	
67	Cho phép tải về tệp tin báo cáo đã được xuất ra	
I.5	**Quản lý tập luật bảo vệ**	
68	Thêm luật mới	
69	Tinh chỉnh luật	
70	Tìm kiếm luật	
71	Xóa luật	
72	Kích hoạt/vô hiệu hóa luật	
73	Xuất tập luật ra tệp tin	
74	Khôi phục tập luật từ tệp tin	
75	Cập nhật tập luật được phát hành bởi nhà sản xuất	
I.6	**Cập nhật tập luật bảo vệ (Thông báo, Tải bản cập nhật các rule từ Extensions)**	
76	Cho phép tự động thông báo có bản cập nhật mới cho quản trị viên	
77	Cho phép tải về trực tuyến và áp dụng thủ công bản cập nhật mới	
I.7	**Quản lý đối tượng được giám sát và nguồn gửi log**	
78	Cho phép quản lý đối tượng được giám sát và nguồn gửi log theo các nhóm được định nghĩa bởi quản trị viên	
79	Cho phép quản lý đối tượng được giám sát và nguồn gửi log theo địa chỉ vật lý, địa chỉ mạng và vị trí địa lý	
I.8	**Quản lý và giám sát tập trung các thành phần tích hợp bên trong**	
80	Cho phép quản lý và giám sát tập trung thông qua giao diện đồ họa các thông số hiệu năng sau của các thành phần tích hợp bên trong: Receiver; Parser; Indexer; Storage; Correlator.	
I.9	**Chia sẻ dữ liệu**	
81	Hệ thống giám sát an toàn không gian mạng quốc gia	
II	**Yêu cầu về kiểm soát lỗi**	
II.1	**Bảo vệ cấu hình**	

82	Trong trường hợp phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), đảm bảo các loại cấu hình sau mà đang được áp dụng phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp: Cấu hình hệ thống; Cấu hình quản trị từ xa; Cấu hình tài khoản xác thực và phân quyền người dùng; Cấu hình tập luật bảo vệ	
II.2	**Bảo vệ dữ liệu log**	
83	Trong trường hợp phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), đảm bảo dữ liệu log đã được lưu lại phải không bị thay đổi trong lần khởi động kế tiếp	
II.3	**Đồng bộ thời gian hệ thống**	
84	Trong trường hợp phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), đảm bảo thời gian hệ thống phải được đồng bộ tự động đến thời điểm hiện tại	
III	**Yêu cầu về log**	
III.1	**Log quản trị hệ thống**	
85	Cho phép ghi log quản trị hệ thống về các loại sự kiện sau: Đăng nhập, đăng xuất tài khoản; Xác thực trước khi cho phép truy cập vào tài nguyên, sử dụng chức năng của hệ thống; Áp dụng, hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình tập luật bảo vệ; Kích hoạt lệnh khởi động lại, tắt hệ thống; Thay đổi thủ công thời gian hệ thống	
86	Cho phép ghi log quản trị hệ thống có các trường thông tin sau: Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây); Địa chỉ IP hoặc định danh của máy; Định danh của tác nhân (ví dụ: tài khoản người dùng, tên hệ thống,…); Thông tin về hành vi thực hiện (ví dụ: đăng nhập, đăng xuất, thêm, sửa, xóa, cập nhật, hoàn tác,…); Kết quả thực hiện hành vi (thành công hoặc thất bại); Lý do giải trình đối với hành vi thất bại (ví dụ: không tìm thấy tài nguyên, không đủ quyền truy cập,…)	
III.2	**Log cảnh báo**	
87	Cho phép ghi log cảnh báo được sinh ra bởi việc thực thi tập luật bảo vệ	
III.3	**Định dạng log**	
88	Cho phép chuẩn hóa log theo tối thiểu 01 định dạng đã được định nghĩa trước để truyền dữ liệu log cho các phần mềm quản lý, phân tích, điều tra log	
III.4	**Quản lý log**	

89	Cho phép thiết lập và cấu hình các cài đặt liên quan đến lưu trữ và hủy bỏ log (ví dụ: ngưỡng giới hạn dung lượng lưu trữ, khoảng thời gian lưu trữ,…)	
90	Cho phép tìm kiếm log theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có)	
91	Cho phép phân nhóm log thành các nhóm sự kiện theo các tiêu chí khác nhau (ví dụ: mức độ quan trọng, các dạng tấn công, các nguồn log,…)	
92	Cho phép truy xuất dữ liệu thô của log thông qua kết quả tìm kiếm và cảnh báo	
93	Cho phép xuất dữ liệu log ra để phục vụ cho việc tích hợp các dữ liệu vào giải pháp khác về quản lý, phân tích, điều tra log	
III.5	**Cách thức tiếp cận log - cho phép tiếp nhận log gửi từ Collector thông qua các cách thức sau:**	
94	Tiếp nhận log qua kết nối UDP	
95	Tiếp nhận log qua kết nối TCP không mã hóa	
96	Tiếp nhận log qua kết nối TCP có mã hóa như TLS hoặc tương đương	
III.6	**Chuẩn hóa log - cho phép tiếp nhận và chuẩn hóa log gửi từ Collector theo tối thiểu 10 loại log khác nhau đáp ứng các yêu cầu sau:**	
97	Chuẩn hóa được log theo các định dạng tệp tin cơ bản tối thiểu với 01 trong các định dạng bao gồm: SYSLOG, JSON, CSV, CEF, NETFLOW	
98	Chuẩn hóa được log của hệ điều hành Windows và Unix	
99	Chuẩn hóa được log của tối thiểu 02 loại tường lửa khác nhau	
100	Chuẩn hóa được log của tối thiểu 04 loại thiết bị mạng khác nhau	
III.7	**Đồng bộ hóa thời gian log**	
101	Cho phép đồng bộ hóa thời điểm log được tiếp nhận tại Receiver và thời điểm log được thu thập tại Collector dựa trên cài đặt về múi giờ đã được thiết lập	
III.8	**Lưu trữ log dưới dạng dữ liệu thô**	
102	Cho phép lưu trữ tất cả log dưới dạng dữ liệu thô bất kể có thể phân tích cú pháp được hay không	
III.9	**Làm giàu thông tin**	
103	Cho phép làm giàu thông tin cho log (ví dụ: phân giải chuỗi ký tự định danh thành tên tài khoản người dùng; lưu lại mốc thời gian sinh log theo múi giờ cục bộ tại máy trạm;…)	

III.10	**Giám sát hiệu năng quá trình tiếp nhận log: cho phép giám sát thông qua giao diện đồ họa các thông số hiệu năng sau của quá trình tiếp nhận log**	
104	Giám sát loại log, thời gian cuối log gửi tới Collector, EPS, ...	
105	Số lượng nguồn log tiếp nhận log không được thực hiện thành công, Error biểu thị số lượng nguồn log không đẩy log tới Collector	
III.11	**Giám sát log tiếp nhận được theo thời gian thực**	
106	Cho phép tạo thống kê dữ liệu theo thời gian thực	
107	Cho phép tìm kiếm và tạo thống kê dữ liệu theo khoảng thời gian xác định	
III.12	**Xử lý thông tin trong log có kiểu dữ liệu địa chỉ IP**	
108	Cho phép xử lý thông tin trong log có kiểu dữ liệu địa chỉ IP tối thiểu theo định dạng IPv4 (ví dụ: xử lý truy vấn tìm kiếm dữ liệu bằng địa chỉ IP,…)	
III.13	**Truyền dữ liệu an toàn**	
109	Cho phép mã hóa dữ liệu hoặc sử dụng giao thức có mã hóa để trao đổi dữ liệu giữa Collector và Receiver	
IV	**Yêu cầu về hiệu năng xử lý: được triển khai thỏa mãn cấu hình tối thiểu theo hướng dẫn cài đặt và thiết lập cấu hình của nhà sản xuất**	
IV.1	**Độ trễ thời gian phản hồi các yêu cầu truy vấn dữ liệu**	
110	Đảm bảo rằng độ trễ thời gian tìm kiếm log với độ phức tạp bất kỳ, có phản hồi trong khoảng thời gian tối đa là 02 phút.	
IV.2	**Xử lý đồng thời nhiều tác vụ: cho phép xử lý đồng thời tối thiểu 03 tác vụ khác nhau đáp ứng các yêu cầu sau**	
111	Cho phép tiếp nhận log theo thời gian thực đồng thời từ tối thiểu 03 nguồn log khác nhau	
112	Có khả năng xử lý đồng thời theo thời gian thực tối thiểu 02 tác vụ cho việc tìm kiếm log và phân tích tương quan sự kiện (ví dụ: nhiều người dùng cùng lúc truy cập và tìm kiếm dữ liệu,…)	
IV.3	**Xử lý đồng thời nhiều sự kiện**	
113	Tối thiểu cho phép xử lý và lưu trữ dữ liệu đồng thời 5.000 sự kiện trong khoảng thời gian là 01 phút	
V	**Yêu cầu về chức năng tự bảo vệ**	

V.1	**Phát hiện và ngăn chặn tấn công hệ thống**	
114	Có khả năng tự bảo vệ, ngăn chặn các dạng tấn công phổ biến sau vào hệ thống (Sử dụng thiết bị WAF): SQL Injection; OS Command Injection; XPath Injection; Remote File Inclusion (RFI); Local File Inclusion (LFI); Cross-Site Scripting (XSS); Cross-Site Request Forgery (CSRF)	
V.2	**Cập nhật bản vá hệ thống**	
115	Cho phép cập nhật bản vá để xử lý các điểm yếu, lỗ hổng bảo mật	
VI	**Yêu cầu về chức năng phân tích tương quan sự kiện và cảnh báo**	
VI.1	**Phân tích tương quan sự kiện theo thời gian thực**	
116	Cho phép phân tích tương quan sự kiện theo thời gian thực đối với dữ liệu log thu thập được	
VI.2	**Phân tích tương quan sự kiện sử dụng danh sách động**	
117	Cho phép phân tích tương quan sự kiện sử dụng thông tin trong danh sách động (ví dụ: tạo luật để so khớp địa chỉ IP, tên miền hoặc giá trị hàm băm đối với một danh sách có thể được cập nhật tự động từ phía nhà sản xuất…)	
VI.3	**Cảnh báo sự kiện giám sát**	
118	Cảnh báo về việc hệ thống ngừng lưu trữ thêm dữ liệu mới khi Storage đã đạt ngưỡng giới hạn lưu trữ mà không thể lưu được dữ liệu mới	
119	Cảnh báo về dấu hiệu, nguy cơ, sự cố, cuộc tấn công và các hành vi gây mất an toàn thông tin khác dựa trên kết quả thực thi luật phân tích tương quan sự kiện	
120	Cho phép sinh cảnh báo chứa các thông tin thuộc nhóm đối tượng được giám sát (ví dụ: cảnh báo về việc có truy cập vào máy chủ email; cảnh báo có truy cập từ xa vào dải địa chỉ IP dành cho các máy chủ…)	
121	Hiển thị nội dung cảnh báo trên giao diện đồ họa về quản lý cảnh báo	
122	Cảnh báo qua phương thức gửi thư điện tử	