هدف شما از این پرامپت چیست؟

- برای گزارش‌گیری، تحلیل خودکار، پاسخ‌دهی سریع (Incident Response)، تولید مستندات، یا آموزش؟

چه نوع ایسیدنت‌هایی مدنظرتان است؟

- مانند: قطع ارتباط، حملات DoS، تغییرات مشکوک در ترافیک، اختلال در DHCP یا DNS، حمله از طریق پورت خاص و غیره؟

می‌خواهید پرامپت چه کاری انجام دهد؟

- تحلیل متن گزارش لاگ‌ها؟ ارائه پاسخ مناسب به ایسیدنت؟ ساخت یک گزارش رسمی؟ تولید خلاصه‌ی حادثه برای تیم امنیتی؟

چه فرمتی برای خروجی مدنظر است؟

- متن ساده؟ فایل جدول‌بندی شده؟ JSON برای ورود به سیستم دیگر؟

با چه سیستم یا ابزارهایی کار می‌کنید؟

- مانند: Cisco Log، Wireshark، ELK Stack، Splunk، Grafana، Zabbix، یا یک سیستم اختصاصی؟

سطح تخصص کاربر نهایی چقدر است؟

- پرامپت برای کاربر حرفه‌ای نوشته می‌شود یا کاربر عمومی/پشتیبانی سطح یک؟