چک لیست معیارهای کلیدی SIEM

آیتم چک‌لیست	معیار	دسته
آیا از دریافت داده‌های بلادرنگ از تمام منابع مرتبط (داخلی، ابری، هیبریدی) پشتیبانی می‌کند؟	تجمیع، نرمال‌سازی و مدیریت لاگ	**قابلیت‌های فنی**
آیا از انواع و فرمت‌های مختلف داده، از جمله فناوری‌های متن‌باز پشتیبانی می‌کند؟		
آیا قابلیت‌های مدیریت لاگ (تجمیع، نمایه‌سازی، نگهداری بلندمدت) مؤثر هستند؟		
آیا قابلیت‌های هوش مصنوعی/یادگیری ماشین برای تشخیص الگوهای پیچیده و کاهش هشدارهای کاذب قوی هستند؟	تحلیل‌های پیشرفته، هوش مصنوعی و یادگیری ماشین(UEBA)	
آیا UEBA برای تحلیل رفتار کاربر و شناسایی ناهنجاری‌ها گنجانده شده است؟		
آیا می‌تواند رویدادهای امنیتی را در چندین سیستم به طور مؤثر همبسته‌سازی کند؟	همبسته‌سازی رویداد و تشخیص تهدید	
آیا قوانین همبسته‌سازی قابل تنظیم و از پیش تعریف شده ارائه می‌دهد؟		
آیا با فیلدهای اطلاعاتی تهدید بلادرنگ یکپارچه می‌شود؟		
آیا هشدارهای بلادرنگ و اطلاعات عملیاتی را برای پاسخ سریع فراهم می‌کند؟	پاسخ به حادثه و خودکارسازی(SOAR)	
آیا شامل الگوریتم‌های پاسخ خودکار به حادثه (مانند مسدود کردن IP ها، قرنطینه کردن) است؟		
آیا با راهکارهای SOAR برای خودکارسازی و هماهنگ‌سازی یکپارچه می‌شود؟		
آیا تجمیع آسان داده‌ها و قابلیت‌های جستجوی زنده برای بررسی فراهم است؟	قابلیت‌های بررسی قانونی	
آیا از نگهداری طولانی‌مدت لاگ‌ها برای تحلیل پس از حادثه پشتیبانی می‌کند؟		
آیا طیف وسیعی از فیدهای اطلاعاتی تهدید را برای شناسایی آسیب‌پذیری‌ها ترکیب می‌کند؟	یکپارچه‌سازی اطلاعات تهدید	
آیا می‌تواند حجم رو به رشد داده‌ها را مدیریت کرده و با نیازهای در حال تحول سازگار شود؟	مقیاس‌پذیری و عملکرد	**جنبه‌های عملیاتی**
آیا گزینه‌های مقیاس‌پذیری شفاف و عملکرد کارآمد را ارائه می‌دهد؟		
آیا با زیرساخت فناوری اطلاعات موجود سازگار است و از API/پلاگین پشتیبانی می‌کند؟	یکپارچه‌سازی و سازگاری	
آیا داشبورد بصری و قابل تنظیم است؟	سهولت استفاده، رابط کاربری و مدیریت	
آیا راه‌اندازی سریع، آموزش کاهش‌یافته و خودکارسازی وظایف را فراهم می‌کند؟		

www.afogtech.ir
شرکت ارتباط افزار افق

آیتم چک‌لیست	معیار	دسته
آیا داشبوردهای متمرکز و گزارش‌های قابل تنظیم برای نیازهای عملیاتی و انطباقی ارائه می‌دهد؟	گزارش‌دهی و داشبوردها	
آیا از استانداردهای انطباقی مورد نیاز (PCI-DSS, GDPR, HIPAA, SOX)پشتیبانی می‌کند؟	پشتیبانی از انطباق با مقررات و نگهداری داده‌ها	**الزامات تجاری و انطباقی**
آیا قابلیت‌های نگهداری طولانی‌مدت داده‌ها را برای حسابرسی فراهم می‌کند؟		
آیا مدل قیمت‌گذاری (اشتراک، به ازای حجم داده، به ازای دستگاه) با بودجه و نیازهای رشد سازمان همسو است؟	مدل‌های هزینه و ساختارهای قیمت‌گذاری	
آیا مدل استقرار پیشنهادی (داخلی، ابری، هیبریدی) با نیازهای کنترل، مقیاس‌پذیری و منابع سازمان مطابقت دارد؟	داخلی، ابری‌محور، هیبریدی	**مدل‌های استقرار**
آیا فروشنده در بازار SIEM شناخته شده و متعهد به نوآوری است؟	شهرت فروشنده و حضور در بازار	**اکوسیستم فروشنده و پشتیبانی**
آیا خدمات حرفه‌ای جامع برای پیاده‌سازی، سفارشی‌سازی و آموزش تیم امنیتی ارائه می‌شود؟	خدمات حرفه‌ای، آموزش وSLA ها	
آیاSLA های واضحی برای پشتیبانی وجود دارد؟		
آیا جامعه فعال کاربران، انجمن‌ها و پایگاه‌های دانش برای پشتیبانی و بهترین شیوه‌ها وجود دارد؟	منابع و پشتیبانی جامعه	
آیا امکان انجام POC برای ارزیابی SIEM در محیط واقعی سازمان فراهم است؟	اهمیت اثبات مفهوم(POC)	

www.ofoghtech.ir
شرکت ارتباط افزار افق