فرآیندها و دستورالعمل‌های SecOps

فرآیند	شرح	چک‌لیست یا اقدامات
مدیریت آسیب‌پذیری‌ها (Vulnerability Management)	شناسایی، ارزیابی، و رفع آسیب پذیری‌ها در سیستم‌ها و نرم افزارها به‌طور مستمر.	☐ انجام اسکن‌های منظم ☐ اولویت‌بندی آسیب‌پذیری‌ها بر اساس شدت ☐ اجرای وصله‌های امنیتی ☐ بررسی اثربخشی رفع آسیب‌پذیری‌ها
مدیریت حوادث امنیتی (Incident Management)	شناسایی، ارزیابی، و پاسخ به حوادث امنیتی به‌صورت سریع و موثر.	☐ تعریف فرآیند شناسایی حوادث ☐ اعلام حوادث به تیم مربوطه ☐ مستندسازی رویدادها ☐ تحلیل اثرات و ارائه گزارش نهایی
نظارت بر امنیت (Security Monitoring)	نظارت مستمر بر تمامی فعالیت های سایبری و نقاط نفوذ احتمالی در سراسر سازمان.	☐ تنظیم سیستم‌های نظارتی ☐ استفاده از SIEM برای تحلیل داده‌ها ☐ هشداردهی خودکار ☐ بررسی و تحلیل رفتار غیرعادی
هوش تهدید (Threat Intelligence)	ارزیابی نوع و پتانسیل تهدیدها برای اجرای بهترین استراتژی‌های امنیت سایبری.	☐ گردآوری اطلاعات تهدید از منابع معتبر ☐ تحلیل اطلاعات تهدید ☐ اولویت‌بندی تهدیدها ☐ اشتراک‌گذاری اطلاعات با تیم‌های مربوطه
ارکستراسیون امنیتی (Security Orchestration) SOAR	ادغام سیستم‌ها و فرآیندهای امنیتی برای مدیریت خودکار و بهینه منابع.	☐ یکپارچه‌سازی ابزارهای امنیتی ☐ تعریف فرآیندهای خودکار ☐ بررسی نتایج و بهبود مستمر ☐ آزمایش سناریوهای امنیتی
تجزیه و تحلیل علت ریشه‌ای (Root Cause Analysis - RCA)	شناسایی علل اصلی رخنه‌ها و نفوذها برای جلوگیری از وقوع مجدد.	☐ تحلیل داده‌های حادثه ☐ شناسایی ضعف‌ها و حفره‌ها ☐ ارائه راهکارهای پیشگیرانه ☐ اجرای اصلاحات لازم