احمدرضا اسدی جوزانی

کارشناس ارشد و سرپرست تیم مرکز عملیات امنیت

متولد: ۱۳۷٤/۰۵/۲۷
وضعیت تأهل: مجرد
وضعیت سربازی: پایان خدمت

خلاصه رزومه

کارشناس ارشد و سرپرست تیم مرکز عملیات امنیت (SOC) با بیش از ۶ سال تجربه در حوزه کشف تهدیدات پیشرفته، واکنش به رخدادها و مدیریت آسیب‌پذیری‌ها. مسلط به مدیریت رویدادهای پیچیده امنیتی، انجام تحلیل ریشه‌ای حوادث و پیاده‌سازی راهکارهای پیشگیرانه برای حفاظت از دارایی‌های حیاتی سازمان. دارای تجربه رهبری تیم‌های چندوظیفه‌ای، آموزش و مربیگری تحلیل‌گران SOC و هماهنگی با ذی‌نفعان برای دستیابی به اهداف امنیتی. متعهد به به‌روز بودن در برابر تهدیدات نوظهور از طریق آموزش‌های تخصصی و اخذ گواهینامه‌های بین‌المللی مانند CCNP Enterprise، CCNP Security، SOC Tier ۲، Fortigate و دوره‌های متنوع SANS.

دوره ها و گواهینامه ها

- CCNP Enterprise
- CCNP Security
- SOC Tier 2
- Fortigate NSE 4 & 7
- Firepower
- SANS SEC542
- SANSSEC560
- SANS SEC573
- SANS SEC503
- SANS SEC511
- SANS SEC555
- SANS SEC504
- SANS SEC450
- SPLUNK FUNDAMENTALS 1 & 2

سوابق تحصیلی

کارشناسی فناوری اطلاعات

دانشگاه حکیم – ۱۳۹۲ تا ۱۳۹۶

سوابق شغلی

سرپرست تیم و کارشناس ارشد SOC

شرکت امن‌افزار گستر شریف – تهران، ایران
تهران
۱٤۰۳ تا الان

وظایف و دستاوردها

- پایش، تحلیل و پاسخ به رویدادها و هشدارهای امنیتی با استفاده از SIEM (Splunk، ELK).
- مدیریت تیم SOC و بهینه‌سازی فرآیندهای پاسخ به رخداد.
- شکار تهدیدات پیشرفته (APT) و حملات بدافزاری و باج‌افزاری.
- توسعه داشبوردها و قوانین شناسایی تهدید.

مشاور امنیت سایبری

شرکت خصوصی
تهران
۱٤۰۳ تا الان

وظایف و دستاوردها

- ارائه مشاوره امنیتی به سازمان‌ها در حوزه راهکارهای دفاعی و کشف تهدید.
- طراحی و پیاده‌سازی سناریوهای آموزشی امنیت سایبری.

مدیر مرکز عملیات امنیت (SOC)

وزارت میراث فرهنگی، گردشگری و صنایع دستی
تهران
۱۴۰۱ تا ۱۴۰۳

وظایف و دستاوردها

- مدیریت عملیات ۷/۲۴ مرکز SOC.
- بهینه‌سازی روندهای اولویت‌بندی و واکنش به رخدادها.
- مربیگری و آموزش تیم تحلیل‌گران SOC.

کارشناس SOC

وزارت میراث فرهنگی، گردشگری و صنایع دستی
تهران
۱۳۹۹ تا ۱۴۰۱

وظایف و دستاوردها

- بررسی هشدارها و تحلیل رویدادهای امنیتی.
- اجرای عملیات شکار تهدید و تحلیل رفتارهای غیرعادی.

کارشناس شبکه

وزارت میراث فرهنگی، گردشگری و صنایع دستی
تهران
۱۳۹٦ تا ۱۳۹۹

وظایف و دستاوردها

- پشتیبانی و مدیریت زیرساخت شبکه سازمان.
- پیاده‌سازی سیاست‌های امنیت شبکه و مانیتورینگ ترافیک.

مهارت‌ها

- پایش و تحلیل رویدادهای امنیتی (SIEM: Splunk, ELK)
- شکار تهدید (Threat Hunting)
- پاسخ به رخدادهای امنیتی (Incident Response)
- خودکارسازی فرآیندهای امنیتی با پایتون
- IDS/IPS (Snort, Suricata)
- EDR و امنیت نقطه پایانی
- امنیت شبکه و فایروال
- تحلیل بدافزار
- چارچوب MITRE ATT&CK

تدریس

- شرکت مهرنا رایانه لیان (آکادمی لیان)
  تهران
  ۱۴۰۳ تا الان

- آموزشگاه پاسارگاد
  تهران
  ۱۴۰۴ تا الان