معرفی

محمد قنبری

بیش از ۹ سال سابقه حضور در پروژه های مختلف امن سازی، امنیت سایبری ، مراکز عملیات امنیت و اسپلانک

تحصیلات دانشگاهی

مقطع	رشته-گرایش	معدل	دانشگاه	عنوان پروژه پایانی	تاریخ اتمام
کاردانی	نرم افزار	۱۷	انقلاب اسلامی تهران	سیستم نرم افزار تحت وب انبارداری	۱۳۹۰
کارشناسی	نرم افزار	۱۶/۵	آزاد تهران شرق	سیستم تحت وب املاک	۱۳۹۳
کارشناسی ارشد	شبکه های کامپیوتری	۱۵	آزاد گرمسار	کاهش توان مصرفی مبتنی بر ایجاد توازن بار در شبکه های ابری با بهره گیری از الگوریتم های فراابتکاری	۱۳۹۷

مقالات و نوشته‌ها

نام	توضیحات	تاریخ	نام
مقاله با عنوان: کاهش توان مصرفی مبتنی بر ایجاد توازن بار در شبکه هاي ابري با بهره گيري از الگوريتم هاي فراابتکاری	لینک مقاله: https://www.civilica.com/Paper-CEITCONF02-CEITCONF02_024.html	۱۳۹۷	مقاله با عنوان: کاهش توان مصرفی مبتنی بر ایجاد توازن بار در شبکه هاي ابري با بهره گيري از الگوريتم هاي فراابتکاری
کتاب با عنوان: راهکارهای پیاده سازی و مدیریت شکار تهدید در سازمان	لینک کتاب : http://mftbook.ir/product/476924	۱۳۹۸	کتاب با عنوان: راهکارهای پیاده سازی و مدیریت شکار تهدید در سازمان
متولی صفحه threat hunting در لینکدین	https://www.linkedin.com/company/threathunting	۱۳۹۸	متولی صفحه threat hunting در لینکدین
متولی صفحه threat hunting در Github	https://github.com/threat-hunting/awesome_Threat-Hunting	۱۳۹۸	متولی صفحه threat hunting در Github
متولی وب سایت SOCLIB.IR Soclib.net	https://soclib.ir https://soclib.net	۱۳۹۹	

دوره های آموزشی و مدارک

عنوان دوره	تاریخ	مدرک
C# ASP.NET	۱۳۹۲	مجتمع فنی ابن سینا
MCITP ,MCSE	۱۳۹۲	مدرک بین المللی ماکروسافت مدرک و مجتمع فنی ابن سینا
CCNA ,CCNP , CCDA , CCNA,CCNP Security (300-206,300-207,300-208, 300-209)	۱۳۹۳-۱۳۹۴	مدرک آموزشگاه رایکا و کایت
دوره تست نفوذ	۱۳۹۴، ۱۳۹۵	آموزشگاه کایت و سازمان فنی حرفه ای
CEH	۱۳۹۴	آموزشگاه کایت، دهکده امن صبا
LPIC1 , LPIC2	۱۳۹۴-۱۳۹۵	لایتک
ITIL Foundation	۱۳۹۶ ، ۱۳۹۷ ، ۱۳۹۸	سازمان فنی حرفه ای -آموزشگاه رایکا و دوران
HP 3PAR , HP Synergy server	۱۳۹۷	آموزشگاه ارژنگ
SANS: 560 , 542	۱۳۹۶	آموزشگاه کاریار ارقام
SNAS: 504,550 , 503 , 511	۱۳۹۷	آموزشگاه کاریار ارقام
Threat Hunting and Threat Intelligence	۱۳۹۷	آموزشگاه کاریار ارقام
Malware Forensic	۱۳۹۸	فناوران توسعه امن ناجی
Splunk 7.X Fundamental Part1	۱۳۹۸	SPLUNK
EC-Council Certified Threat Intelligence Analyst	۱۳۹۸	مدرک بین المللی شرکت EC-Council
Cyber Threat Hunting	۱۳۹۹	Active Countermeasures
Active Defense & Cyber Deception	۱۳۹۹	Black Hill, Active Countermeasures
Autopsy	۱۳۹۹	BASIS Technology
Fortinet NSE1, NSE2	۱۳۹۹	Fortinet
SPLUNK Admin,ES,UBA,Phantom	۱۳۹۸-۱۴۰۱	Self study
Splunk Core Power user	۱۴۰۱	Splunk Certificate

مهارت‌ها

- مسلط به مفاهیم، و استراتژی های Threat Hunting و Threat Detection
- مسلط به راهکارهای استقرار و پیکربندی NSM و راه حل های Threat Detection and Hunting در سازمان
- مسلط به پیاده سازی و پشتیبانی SPLUNK
- مسلط به طراحی Appهای SPLUNK
- مسلط به طراحی و توسعه Rule و Use Case
- آشنا با راه اندازی و کار با ELK
- مسلط به تشخیص تهدیدات مبتنی بر MITRE ATT&CK Framework
- اشنا به مفاهیم Red Team & Blue Team
- مسلط به تحلیل حوادث امنیتی و لاگ تجهیزات Cisco،Fortinet، Juniper، HP،آنتی ویروس و سیستم عامل های لینوکس و ویندوز
- مسلط به طراحی LOM سخت افزار مناسب با نیازمندیهای موجود
- مسلط به راه اندازی و پیکربندی سرور و ذخیره سازهای HP مانند DL و BL و Synergy، 3PAR و MSA

تجربه

- تجربه راه اندازی و کار با ابزارهای ، OSSEC، sysmon، Osquery، splunk، Bro IDS، Suricata
- تجربه استقرار و نگهداری SPLUNK
- تجربه استقرار و نگه داری تجهیزات سروری HP و ذخیره سازی HP 3PAR
- تجربه استقرار پیکربندیCisco ISE , Firepower
- تجربه طراحی شبکه مطابق معماریCisco safe
- تجربه استقرار، پیکربندی و پشتیبانی فایروال ASA و Fortigate
- تجربه استقرار، پیکربندی و پشتیبانی نرم افزارهای مانیتورینگ از قبیلManage Engine, Zabbix, Solarwinds
- تجربه استقرار، پیکربندی و پشتیبانی نرم افزارهای پشتیبان گیری از قبیلBackupExec, Veeam
- تجربه کار با ابزارهای Empire , Metasploit, Nmap, Nessus
- تجربه راه اندازی محیط مجازی مبتنی بر VmWare با قابلیت هایFT , HA, Clustering
- تجربه استقرار، پیکربندی و پشتیبانی دامین ویندوز در حوزه های بزرگ
- تجربه کار با ذخیره ساز Tape Tandberg
- تجربه استقرار، پیکربندی و پشتیبانی SCCM وSCOM
- تجربه های متعدد برنامه نویسی با C# ، ASP.NetوMS SQ

سوابق شغلی

نام شرکت و سازمان	موقعیت سازمانی	تاریخ
شرکت رایموند	کارشناس شبکه	۱۳۹۱-۱۳۹۲
شرکت پژند الکترونیک (تمام وقت): - گروه بهمن - مجمع تشخیص مصلحت نظام	**گروه بهمن** - Network and System Admin - کارشناس امنیت **مجمع تشخیص مصلحت:** - کارشناس پروژه امن سازی مجمع تشخیص مصلحت نظام - Network and System Admin	۱۳۹۳-۱۳۹۴
شرکت زیرساخت امن خدمات تراکنشی - بانک ملت	**مرکز عملیات امنیت بانک ملت** - Security & Data Engineer - مدیر پروژه Threat Hunting - SIEM Content Developer - Splunk Architecture	۱۳۹۵-۱۳۹۹
- شرکت پایه ریزان فناوری هوشمند	- مدیر بخش امنیت و سرویس های SOC و SPLUNK ○ مشاور و مدیر پروژه SOC شرکت تجارت الکترونیکی **ارتباط فردا** (PSP) ○ مشاوره و مدیر پروژه SPLUNK **بانک رسالت** ○ مشاوره و مدیر پروژه SPLUNK **بانک اقتصاد نوین** ○ مشاوره و مدیر پروژه SPLUNK **شرکت یاس ارغوانی**	۱۴۰۱-۱۳۹۸
- پلیمرآریا ساسول	- پیاده سازی اسپلانک + ES	۱۴۰۰-۱۳۹۹

✓ گروه مپنا (توسعه ریلی)	✓ مشاور مرکز عملیات امنیت و اسپلانک	۱۳۹۹-۱۴۰۰
✓ شرکت توسعه راه امن	✓ مدیر فنی ✓ مالک استارت اپ TDLIB	۱۳۹۹-۱۴۰۰
✓ شرکت گل گهر سیرجان	✓ مشاور SOC و SPLUNK	۱۳۹۹-۱۴۰۰
✓ شرکت توسعه فناوری سوشیانت	✓ مشاور SOC و SPLUNK	۱۴۰۰-۱۴۰۱
✓ هلدینگ ارنیکا	✓ مدیر SOC و NOC	۱۴۰۰-۱۴۰۱
✓ **شرکت ویستا سامانه آسا**	✓ مشاور SOC و SPLUNK	۱۴۰۰
✓ **شرکت Savola**	✓ مشاور SOC و SPLUNK	۱۴۰۰
✓ **شرکت نوآروان دوران**	✓ مدرس دوره های اسپلانک	۱۴۰۱
✓ **شرکت خودرو سازی کروز**	✓ مشاور SOC و SPLUNK	۱۴۰۱
✓ **شرکت اک تک تکنولوژی کیش**	✓ مشاور SOC و SPLUNK	۱۴۰۱
✓ **بانک ملت**	✓ مشاور SOC و SPLUNK	۱۴۰۱
✓ **بانک سامان**	✓ مشاور SOC و SPLUNK	۱۴۰۱