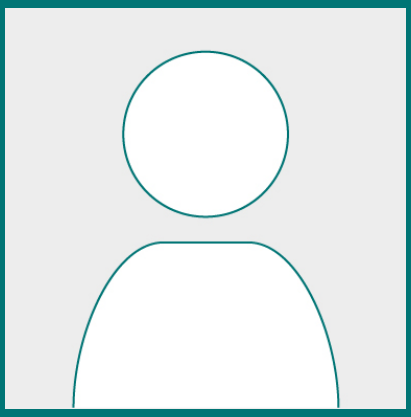


علیرضا کتانی

متولد: ۱۳۷۹/۱۲/۰۳

وضعیت تاهل: **مجرد**

وضعیت نظام وظیفه: **معافیت**

درباره من

من علیرضا کتانی، فارغ التحصیل مهندسی کامپیوتر کارشناسی و کارشناسی ارشد از دانشگاه صنعتی اصفهان هستم.در طول فعالیت حرفه‌ای خود در پروژه‌های مختلف SOC، با سامانه‌های SIEM و ابزارهای شبیه‌سازی حملات نظیر Caldera، Burp Suite و Atomic Red Team کار کرده‌ام و از آن‌ها برای ارزیابی توانایی تشخیص حملات، اعتبارسنجی قوانین امنیتی و بهبود فرآیندهای کشف تهدید استفاده کرده‌ام. در این رابطه برای درک بهتر حتما پیوست با نام ELK.pdf و fardad.pdf واقع در همین مستند خوانده شود.

همچنین در دوران دانشگاه با مفاهیم مهندسی معکوس و تحلیل نرم‌افزار آشنا شدم و تجربه کار با ابزارهایی مانند IDA Pro، Ghidra و Objdump را کسب کردم. در چند پروژه محدود نیز به تحلیل و کرک نرم‌افزارها پرداخته‌ام، هرچند حوزه اصلی تخصص من عملیات امنیت و تشخیص تهدیدات است.

در حوزه زیرساخت، طی دو سال فعالیت در مرکز آپای دانشگاه صنعتی اصفهان با Kubernetes، Docker، Ansible، Grafana و Prometheus کار کرده‌ام. همچنین در پروژه‌های مانیتورینگ امنیتی زیرساخت‌های Kubernetes، ابزارهایی نظیر Tetragon را برای جمع‌آوری و تحلیل رویدادهای امنیتی به همراه Splunk به‌کار گرفته و در زمینه پایش منابع و سلامت زیرساخت فعالیت داشته‌ام.

در مقطع کارشناسی ارشد نیز بر روی پروژه خودکارسازی فرآیند پاسخ به رخدادهای امنیتی با استفاده از AI Agentها فعالیت کرده‌ام. در این پروژه از فناوری‌هایی نظیر LangChain و RAG استفاده کرده و همچنین یک مدل Phi3.5 را با استفاده از داده‌های گردآوری‌شده از منابع مختلف فاین‌تیون کرده‌ام.

سوابق شغلی

کارشناس زیرساخت SOC

دی ۱۴۰۴ - تاکنون

ایریسامستقر در SOC مجتمع فولاد مبارکه

مسئولیت SOC Tier2 در SOC فولاد مبارکه- تیونینگ رول‌های ES- کانفیگ کامل Data model های برای FP و همچنین فیلدهای unknown- استخراج فیلدها با Regex، موارد Field Aliasation، تگ گذاری لاگ‌ها و...

مدیریت زیرساخت کلاستری خود اسپلانک برای اطمینان از صحت کارکرد آنها- اصلاح مشکلات بین روابط اینستنس های مختلف- تخمین زیرساخت مورد نیاز سه ماهه برای عناصر جدید اضافه شده به سیستم-تسلط کامل به فرایند ارسال لاگ از مبدا Agent به سرورهای ایندکسر و همچنین فرایند سرچ در سرچ هد برای رفع مشکلات- تسلط کامل بر تک تک المان های زیرساخت کلاستر شامل Search head,cluster master,deployment server-indexer-HF,UF,Deployer- تسلط بر انواع ورودی گرفتن لاگ نظیر HTTP Colletor, OTel Collector و ...- تسلط بر لاگ گیری سمت شبکه توسط ایجنت خود اسپلانک Splunk streamer و Zeek-

تهیه گزارش‌های ماهانه مدیریتی- نصب APP های و addon های جدید منتسب با ابزارهای جدید نظیر Palo Alto، FTDو ...-تغییر کانفیگ addon ها مبتنی بر فایل و مبتنی بر وب برای مواردی که Addon کانفیگ نادرستی دارد- ایجاد Addon برای لاگ‌های پلتفرم‌های بومی و همچنین سامانه‌هایی که addon داخل خود اسپلانک ندارند.

ایجاد کوئری‌های تشخیص حملات جدید متناسب با گزارش‌های Hacker NEWS و CISA NEWS- فارنزیک مبتنی بر لاگ و همچنین مبتنی بر ابزار نظیر Kape- بررسی حوادث گزارش داده شده توسط SOC Tier1 شیفت عصر و شب و بستن آنها-

پژوهشگر LLM

مهر ۱۴۰۲ - شهریور ۱۴۰۴

دانشگاه صنعتی اصفهان

در شهریور ۱۴۰۴ پایان‌نامه کارشناسی خود را با موضوع طراحی و پیاده‌سازی SOC هوشمند مبتنی بر

راه های ارتباطی

نجف آباد

۰۹۳۳۷۹۳۰۳۸۳

alirezakatani1379@gmail.com

alreka1379@gmail.com

www.linkedin.com/in/alireza-katani-61bba919b

فایل ضمیمه رزومه

f3db80f1-1989-479e-8001-5edf9194534e.pdf

کارشناس SOC و اجرای SIEM

اسفند ۱۴۰۲ - شهریور ۱۴۰۳

سپاهان دانه

از سمت مرکز آپا به عنوان کارشناس SOC شرکت سپاهان دانه مشغول به انجام پروژه شدم. در این راستا نصب و تیونیگ Splunk ES از صفر تا صد برعهده داشتم. همچنین پیاده سازی use case های مبتنی بر MITRE ATT&ck و متناسب با پلتفرم ها و نوع تجارت سازمان برعهده ام بود. این یکی از پروژه های من در زمان مشغول به کار در مرکز اپا بود.

کارشناس soc

تیر ۱۴۰۱ - شهریور ۱۴۰۱

فرداد

به مدت سه ماه به عنوان کارآموز در شرکت فرداد مشغول به کار شدم.در این مدت به مبانی SIEM,SOC تسلط پیدا کردم.در این مدت با فریمورک SPLUNK در ترکیب با misp,zeek,suricata,sysmon به تشخیص برخی از حمله ها پرداختم. در مستند پیوست شرح تمامی کارها موجود میباشد.

fardad.pdf

کارشناس soc

مهر ۱۴۰۲ - تیر ۱۴۰۴

پژوهشکده اپا

کارشناس زیرساخت و امنیت

مهر ۱۴۰۳ - شهریور ۱۴۰۴

آپا

LLM و AI Agentها به انجام رساندم. هدف این پروژه، خودکارسازی تحلیل و پاسخ به رخدادهای امنیتی و کاهش وابستگی به SOC Tier 1 و Tier 2 بود. در این راستا، یک مدل زبانی مبتنی بر دیتاست اختصاصی توسعه داده شد و با استفاده از LangChain و LangGraph به عامل‌های هوشمند برای تحلیل و پاسخ‌دهی خودکار مجهز گردید. همچنین برای همبستگی و زنجیره‌سازی حملات مبتنی بر MITRE ATT&CK از معماری RAG، پایگاه داده برداری ChromaDB و ذخیره‌سازی تاریخچه رخدادها استفاده شد. این پروژه موجب کسب تجربه عملی در حوزه هوش مصنوعی، یادگیری ماشین و LLMها، شامل Deep Learning، معماری‌های Transformer نظیر BERT و LLaMA، فاین‌تیون مدل‌ها با روش‌های SFT، LoRA و QLoRA، استفاده از Hugging Face، PEFT، PyTorch و Scikit-Learn شد. نتایج پژوهش منجر به انتشار یک مقاله علمی شده و مقاله جامع پروژه پس از ارزیابی در محیط عملیاتی منتشر خواهد شد.

Finaldoc_for print.pdf

IEEE article_V4.pdf

سوابق تحصیلی

مهندسی کامپیوتر — دانشگاه صنعتی اصفهان

مقطع : کارشناسی ارشد

مهر ۱۴۰۲ - شهریور ۱۴۰۴

مهندسی کامپیوتر — دانشگاه صنعتی اصفهان

مقطع : کارشناسی ارشد

مهر ۱۳۹۸ - شهریور ۱۴۰۲

مهارت ها

- MITRE ATT&CK
- Sigma Rules
- wazuh
- Splunk
- Sysmon
- Linux
- تحلیل لاگ‌های Fortigate
- Purple Team
- Sans504
- Sans450
- کانفیگ Waf modsecurity و تحلیل لاگ آن
- lang grah
- promethusgr afana
- chainsaw
- Snort، Suricata، Zeek
- ELK Stack
- Blue team operations
- Wireshark
- CCNA
- FortiwebWAF
- Python
- Active Directory
- sans401
- Ansible
- Docker
- alert manager

Kubernetes

اشنایی و کار با Nessus

Caldera

poshc2

Splunk Attack Range

BURP SUIT

atomic red team

Red team

LLM

rag

AI Agents Development ((n8n

Lang chain

HuggingFace

IDA Pro

ghidra

obj dump

Kape

زبان ها

انگلیسی

گواهینامه ها و دوره ها

دوره LLM سایت Hugging Face

Hugging Face

png.2025-03-06

صدور: آبان ۱۴۰۴

دوره Purple Team راوین

راوین

در حال شروع برای دیدن ویدیوها و گرفتن Cert

دوره CCNA و MCSA

ITSheild

دوره رایگان توسط اقای اخزری منتشر شده.

دوره Sans 504

ITsheild

دوره هوش مصنوعی روبوتک

روبوتک

تنها مبحث شبکه های بازگشتی و LLM ها رو دیدم

دوره هوش مصنوعی

هوسم

صدور: شهریور ۱۴۰۴

تمامی مباحث دوره رو توانستم ببینم

دوره CEH جادی

صدور: فروردین ۱۴۰۰

مکتب خونه

بدون گواهی صرفا دیدن فیلمها

دوره مبانی برنامه نویسی کوئرا

کوئرا

برنامه نویسی پایتون، سی و جاوا

C-Cert.jpg

دوره SOC سورین (تحلیلگر سورین و توسعه دهنده)

150 ساعت دوره شامل روند دقیق تحلیل حملات براساس ابزارهای SOC

دوره بدون گواهینامه بوده اما میتوانید مباحث آن را در پیوست مشاهده کنید.

Soorian.pdf

دوره SOC Tier1

لیان

خرید به صورت اشتراکی

دوره SOC Tier2

لیان

خرید به صورت اشتراکی

دوره کوبرنتیز

انیسا

در حال گذراندن دوره کوبرنتیز انیسا

دوره متخصص Splunk و Splunk ES

صدور: تیر ۱۴۰۴

اکادمی راوین

در 16 تیر 1404 دوره Splunk ES رو با موفقیت گذراندم.

Cert.pdf

پروژه ها

ایجاد سرور SIEM و تشخیص حملات APT با استفاده از ELK

تاریخ: ۱۴۰۲

مسئول و تهیه کننده پروژه

در پروژه کارشناسی، حمله APT29 با استفاده از ابزارهای PoshC2 و Caldera بر اساس تکنیک‌های MITRE ATT&CK شبیه‌سازی و اجرا شد. برای پایش و تشخیص حملات، زیرساخت ELK Stack به همراه Wazuh پیاده‌سازی گردید که شامل یک سرور C2، یک سرور مانیتورینگ و دو سیستم قربانی (ویندوز و لینوکس) بود. تشخیص مراحل مختلف حمله از طریق قوانین Wazuh و نگاشت آن‌ها به تکنیک‌های MITRE انجام می‌شد و با زنجیره‌سازی تکنیک‌ها، فازهای کامل حمله شناسایی می‌گردید. فایل پیوست خوانده شود.

ELK.pdf

پیمانکار و اجرا کننده SOC پیاده‌سازی صفر تا صد مبتنی بر اسپلانک در کارخانه بیسکوییت فرخنده

تاریخ: ۱۴۰۴

در شهریور ماه سال 1404 به وسیله قرارداد پیمانکاری مسئول پیاده سازی صفر تا صد SOC مبتنی بر اسپلانک در کارخانه بیسکوییت فرخنده شدم. در این راستا از تمام تجربه‌های قبلی برای پیاده‌سازی ابزارهای مانیتورینگ استفاده کردم. در نهایت اسپلانک به صورت کلاسترینگ به همراه ابزارهای zeek,suricata, ... در ساختار داکری پیاده‌سازی شد. در مرحله بعد تست نفوذی به وسیله ابزارهای nessus برای تست وب و همچنین atomic red team برای تشخیص و دفاع در اسپلانک پیاده‌سازی شد.

کارشناس پیاده سازی مانیتورینگ امنیتی و زیرساختی کوبرنتیز

تاریخ: ۱۴۰۴

مسئول لاگ‌گیری و مانیتورینگ Kubernetes در رویداد CTF مرکز آپا؛ جمع‌آوری لاگ‌ها با Tetragon، ارسال به Splunk از طریق OpenTelemetry، پیاده‌سازی مانیتورینگ متریک‌ها با Prometheus و Grafana، و پیکربندی و تحلیل زیرساخت Kubernetes و ابزارهای امنیتی مرتبط. مرکز آپا

کارشناس خودکار سازی نصب Splunk و App های مورد نظر به وسیله ansible

تاریخ: ۱۴۰۴

برای نصب و خودکار سازی نسب splunk و App های مربوطه داحل محیط کوبرنتیز و همچنین سایر Agent ها از انسیبل استفاده شد. در کنار این موضوع کار با داکر و همچنین نصب اسپلانک در محیط داکری را نیز تجربه کردم. مرکز آپا

کارشناس SOC توسعه زیرساخت SIEM دانشگاه صنعتی اصفهان برمبنای Splunk

تاریخ: ۱۴۰۴

کارشناس پیاده‌سازی SIEM مبتنی بر Splunk در دانشگاه صنعتی اصفهان-Splunk به صورت کلاسترینگ نصب شده و در نهایت به وسیله Splunk ES قوانین تشخیص حملات فعالسازی و تیون شد. در این راستا ابزارهای لاگ‌گیری Zeek ، sysmon؛ suricata بر روی سرورهای مجزا نصب و کانفیگ شد و در نهایت لاگ آنها در سمت اسپلانک مورد بررسی قرار گرفت. برای پلتفرم هوش تهدید از قابلیت هوش تهدید خود سامانه Splunk به همراه نصب و کانفیگ سرورMISP استفاده شد. لاگ گیری از اکتیو، کلاینتها و فایروال FTD نیز انجام شد. مرکز آپا

دانشجو پروژه های توسعه امن نرم افزار

تاریخ: ۱۴۰۴

در درس امنیت توسعه امنیت نرم افزار، در فصل اول با حملات سمت وب نظیر Sql injection،XSS,File Upload,Remote File Execution به صورت عملی آشنا شدیم. در فصل دوم با حملات Buffer Over Flow و همچنین انواع روش های دور زدن مکانیزم های امنیتی نظیر Canary آشنا شدیم. در فصل سوم با انواع روشهای مهندسی معکوس و کرکینگ به وسیله نرم افزارهای Ghidra,Hex Dump,Ida pro, obj

dump آشنا شدم و چند نمونه ساده از کرکینگ برنامه ها رو انجام دادیم.

تست هوش ریون

تاریخ: ۱۴۰۴

آزمون دهنده

تست هوش ریون کاربوم

تست ریون

افتخارات و جوایز

رنک 1 کارشناسی ارشد مهندسی کامپیوتر

تاریخ: ۱۴۰۴

رنک 1 کارشناسی مهندسی کامپیوتر سال 1405

رنک 4 کارشناسی مهندسی کامپیوتر

تاریخ: ۱۴۰۲

رنک 4 کارشناسی مهندسی کامپیوتر با معدل 18.21 در دانشگاه صنعتی اصفهان

فعالیت های داوطلبانه

TA

تاریخ: ۱۴۰۴

یک ترم همیار درس توسعه امن نرم افزار

سر تی ای درس توسعه امن نرم افزار- تهیه انواع تمـــــــارین Sql injection, buffer over flow,xss و همچنین Reverse Engineering و ...

Teaching assistant

تاریخ: ۱۴۰۰

یک ترم همیار درس Data Mining

Teaching assistant

تاریخ: ۱۴۰۴

همیار درس امنیت شبکه دکتر منشی

یک ترم سر TA درس امنیت شبکه دکتر منشئی