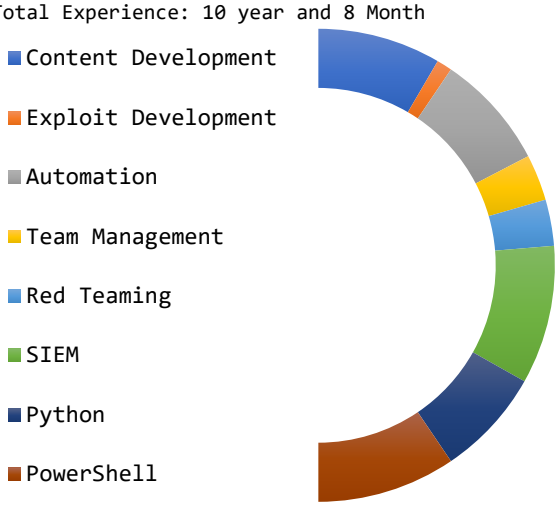
Gurmukhnishan Singh

Email : gurmukhnishansingh@gmail.com
Phone No : +916005122291
Location : Bangalore

LinkedIn
GitHub
Twitter
Website

Profile Summary

Total Experience: 10 year and 8 Month

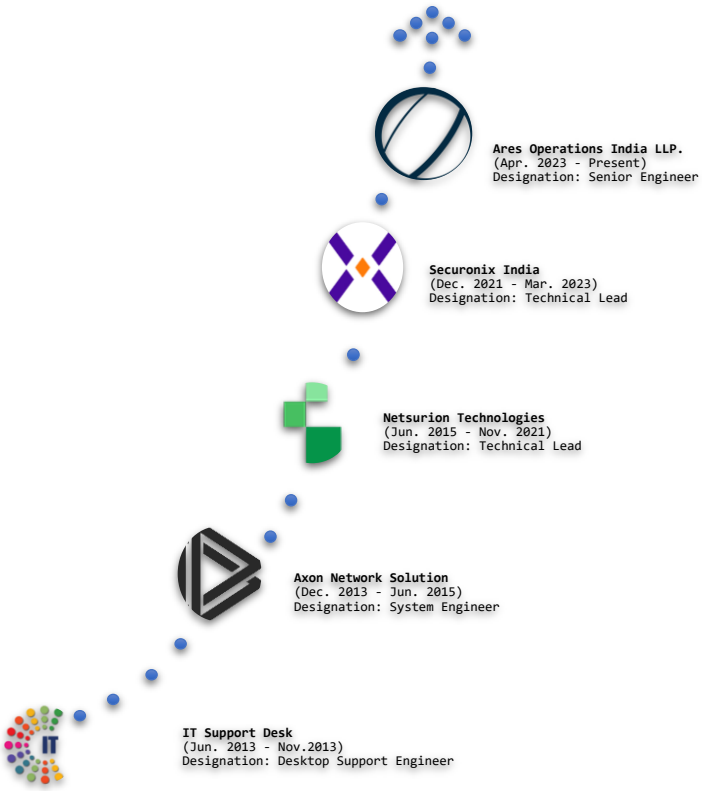


- Result oriented professional with more than 10 years of experience across Infrastructure Technologies, **Cybersecurity**, and **Development**.
- Skilled in **PowerShell**, **Python**, **JavaScript**, **SIEM Content Development**, **Tools Development**, **Data visualization** and **Exploit Development**.
- Hands-on experience on Cybersecurity technologies like **SOAR**, **UEBA**, **SIEM**, **Sandboxing**, **MITRE ATT&CK framework**, **Malware Analysis**, **Log Monitoring**, **Log correlation** and many more.
- Excels in assessing Cybersecurity requirements & translating these into techno-functional specifications; providing designing solutions & troubleshooting information systems.
- Insightful knowledge of Information Security Compliance and Risk Assessment Methodologies.
- I have ability to motivate and lead the team to achieve common goal.

Projects

Following are some majors' projects I have developed and execution in my career:

- Netsurion SIEM connectors for following technologies:
  - Microsoft 365 Suite
  - Amazon web Services
  - Microsoft Azure
- Jupyter Notebook Integration with Netsurion SIEM.
- MITRE ATT&CK Framework Integration with Netsurion SIEM.
- Remote Workforce Security
- Advance correlation scripts for Netsurion SIEM (like Simultaneous login, kerberoasting, password spraying, etc)
- Vulnerability assessment integration with Netsurion SIEM
- More than 50 product integration with SIEM
- Content portal for Securonix SIEM.
- Content Validation framework (Salus) for Securonix SIEM.
- Revamping of Securonix ATS (Autonomous threat Sweep)
- Detection as a Code using SVN and Jenkins.
- Written Exploit for downloading malicious content using Windows Native API.
- XSOAR Playbook – Phishing and external indicator blocking
- XSOAR BYOI – Abnormal security, internal IP address and domain integration.

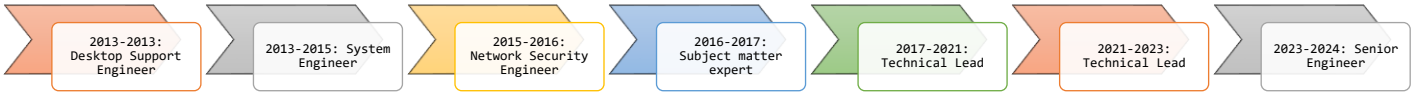


Education & Certifications

- **2012**: B.E from Jammu University
- **2008**: H.S.C from JKBOSE
- **2006**: S.C from JKBOSE

- ATT&CK Defender Cyber Threat Intelligence Certification
- ATT&CK Defender Security Operations Center Assessment Certification
- Certified SNYPR Content Developer, Data Integrator and Security Analyst

Growth Path



Work Experience

March 2023 – Present: Ares Operations India LLP as Senior Engineer

Roles and responsibilities:

As a Senior Security Engineer at Ares Management, I led critical aspects of the security operations, focusing on automation, threat intelligence, and incident response to bolster organizational security posture. My key responsibilities and achievements included:

Incident Response and Automation:

- Spearheaded the deployment and management of the **XSOAR** platform, enhancing the automation of incident response playbooks and custom integrations.
- Developed and maintained an array of **Bring Your Own Integrations** (BYOI) solutions, including **abnormal security**, **Splunk attack analyzer**, and **internal domain/IP address integrations** with XSOAR threat intelligence.
- Crafted and refined playbooks for efficient **phishing response**, **indicators of compromise (IoC) blocking**, and the ongoing maintenance of existing automation workflows.

Threat Intelligence and Security Analytics:

- Managed the **Splunk platform and CrowdStrike**, focusing on the creation and continuous improvement of threat-related **alerts, dashboards, and reports**. This initiative significantly eased the **threat hunting and daily operational tasks** for the SOC team.
- Innovated in the development of **custom scripts** to streamline team operations, including automating the retrieval of **MAC tables from switches** to aid in **network mapping and insider attack** detection.

Data Integration and Management:

- Oversaw the integration of new data sources and the management of existing products through **Cribl**, ensuring seamless **data ingestion and optimization for security analysis and operations**.

Operational Efficiency and Team Support:

- Authored custom scripts and tools aimed at simplifying and expediting team tasks, thereby enhancing overall operational efficiency and enabling quicker response to security incidents.

Cross-functional Collaboration and Leadership:

- Collaborated closely with cross-functional teams to identify, assess, and mitigate security risks, driving continuous improvement in the organization's security framework.
- Played a pivotal role in mentoring junior team members and contributing to the development of a knowledge-sharing culture within the security operations team.

December 2021 – 03 March 2023: Securonix India PVT. LTD. as Technical Lead

Experience: 1 year and 4 months

Roles and responsibilities:

- Compromising the target lab machine by extracting information, infiltrating its system via various red teaming tools like **Caldera, Picus and AttackIQ**.
- Changing the attack code and artefacts to avoiding detection by the blue team and making it extremely tricky for the blue team to neutralise the threat before the damage is done.
- Exploiting bugs and weaknesses in the lab environment to highlight the gaps in the detection content to improve detection cover.
- Develop, improve and maintain reporting metrics and mechanisms used to make decision and measure detection content quality, efficiency and responsiveness.
- Managing a team and/or workstream on an engagement, staying educated on current trend and assisting in the development of knowledge capital.
- Sets team direction; oversees work activities of engineers; providing forecasting and planning input.
- Lead automation projects including all administrative and execution efforts which helps engineer to provide good **quality detection content**.
- Lead **detection engineering** projects including development and deployment efforts for providing actionable and good quality detection content.
- Coordinates with other managers to help understanding and solving issues related to detection contents.
- Managing and/or contributing to project planning, engagement administration, and successful completion of engagement workstream(s).
- Monitoring SME, ensuring they stay up-to-date on improvement and development in **detection content**.
- Develop, improve and maintaining **content validation framework** which helps finding issues automatically from existing and new content.
- Develop, improve and maintaining **content portal** which helps exposing policies, threat model and parser to stakeholder.
- Lead **autonomous threat sweep development** effort for providing optimised, improved and scalable product.
- Utilize the SCRUM agile development methodology as a product owner and SCRUM Master.

- Reviewing PR from junior developer to find bugs and issues in code.
- Help defining project scope, goals and deliverables.
- Developing pre-commit scripts to find known bugs in content and automation scripts commits.

June 2015 – December 2021: Netsurion Technologies PVT. LTD. as **Technical Lead**
Experience: 6 year and 5 months
Roles and responsibilities:

- Developing solution for monitoring security, operation and compliance (**PCI DSS, HIPAA, FISMA**, & so on)
- Implementing **integration scripts & tools** for fetching logs from on-perm, cloud and DB based devices using **Python, PowerShell, Bash, API, EventHub, S3**, & so on.
- Generating Use Cases which SOC need to monitor for finding suspicious activities happening on client environment.
- Mentoring & supporting other members of the team to assist in completing tasks and meet objectives.
- Coordinating with SOC, Supports and Sales Team for understanding client requirement and accurate implementations of security products.
- Publishing details about our work by writing uses cases blogs, integration guide and details about knowledge packs over websites which helps customers to understand needs and usage of solution.
- **Writing rules for MITRE ATT&CK techniques and procedures** to detect adversaries' activities in customer environment.
- Delegating development & implementations work among other teams' members.
- Collaborating with internal development, testing and support teams for making product better and solving customer challenges.
- Developed **IR playbooks** for automate the tedious process of analysing and enrichment of incident.
- Managing, developing and supporting integration of SOAR with ticketing platform, external enrichment tools like **VT, DNSBL, SPAM analysers, SIEM**, etc.
- Writing and reviewing rules for MITRE ATT&CK techniques and procedures to detect adversaries' activities in customer environment.
- Executing **fine tuning of alerts**, MITRE ATT&CK technique detection rules for reducing the false positives
- Detecting malicious process using **Cuckoo Static and Dynamic Analysis** on memory dump or process sample

June 2013 – June 2015: Previous Experience

- **Axon Network Solutions PVT. LTD** as **System Engineer** (**November 2013 – June 2015**) 1 year and 8 months
- **IT Support Desk** as **Desktop Support Engineer** (**June 2013 – November 2013**) 6 months

Technologies/Tools Used

- Elasticsearch
- Graphana/Kibana
- Netsurion SIEM
- Securonix SIEM
- Python/PowerShell
- JavaScript
- SQL/GIT/SVN
- Jupyter Notebook
- SOAR
- UEBA
- Log Correlation
- Regular Expression
- Caldera
- Atomic Red Team
- MITRE ATT&CK Navigator
- Wireshark/Tshark

Declaration

I solemnly declare that all the above information is correct to the best of my knowledge and belief.

Date :
Place : Bangalore

Gurmukhnishan Singh