AKSHAY SURYAWANSHI

Lead Information Security Engineer

+91 9702891380 | akshay.suryawanshi@hotmail.com | Linkedin Profile | Portfolio | Mumbai

SUMMARY

Lead Information Security Engineer with 8+ years of progressive experience across Incident Response, Digital Forensics (DFIR), SOC Operations, Vulnerability Management, Threat Intelligence, Cloud Security (AWS, Azure, OCI) and GRC. Proven expertise in IR planning, forensic investigations, SOC workflow automation, threat mitigation, and enterprise security hardening across hybrid and multi-cloud environments. Skilled in securing data in transit, at rest, and in use while strengthening application, API, and infrastructure security.

Brings a strong foundational background in on-premises, virtualized, and cloud infrastructure, enabling the ability to bridge IT and Security, align technical controls with governance requirements, and lead cross-functional engineering collaboration. Recognized for driving security architecture improvements, operational excellence, and delivering measurable risk reduction across global environments. Committed to continuous learning with relevant certifications and active engagement in cybersecurity research, tools, and emerging threat trends.

EXPERIENCE

03/2024

Mumbai

Lead Information Security Engineer (Acting Team Lead)

Cimpress India Private Limited

Leading security engineering team for the National Pen business unit

- Built an AI-driven L1 SOC triage workflow integrating CrowdStrike, VirusTotal, ChatGPT, Power Automate, and Jira-reducing manual investigation workload by ~50% and accelerating response times.
- Established an in-house Digital Forensics & Incident Response (DFIR) lab to support deep forensic investigations, malware analysis, and faster containment of security incidents.
- Created NIST-aligned Incident Response Plan, defining roles, workflows, escalation paths, improving incident response maturity.
- Deployed Flare.io, Cyble, Google Threat Intelligence to enhance IOC enrichment, darknet visibility, exposure monitoring, and proactive threat identification.
- Coordinated external penetration tests, validated findings, and led remediation across application and cloud infrastructure environments.
- Developed phishing simulations with Microsoft Defender. Launched phishing awareness training via LMS to reduce user susceptibility and enhance security culture.
- Owned vulnerability management lifecycle by prioritizing findings using CVSS, asset criticality, and exploitability, driving timely remediation across infrastructure, cloud, and applications.
- Executed email and data retention policies aligning with regulations, enhancing compliance and reducing risk.
- Performed threat modeling and architecture security reviews for AWS/OCI. Analyzed IAM, network, compute, storage, APIs, monitoring, and public-facing services, achieving multi-cloud attack surface reduction.
- Performed end-to-end firewall and network security reviews across on-prem and cloud environments, validating ACLs, SSL/TLS settings, NAT policies, segmentation, and threat-prevention controls.
- Led the migration from LastPass to Keeper for ~3,000 employees, ensuring secure rollout, user onboarding, and infrastructure integration.
- Driving the security roadmap in alignment with security standards, business risk appetite, and regulatory requirements, ensuring consistent security posture across global environments.
- Partnering with Engineering, SRE, Cloud, IT, Legal, Privacy, and Audit teams to align security controls with business objectives and delivery timelines.
- Establishing and governing risk registers, risk acceptance workflows, third-party security assessments, and audit readiness activities aligned with ISO 27001, CIS Controls, and NIST CSF.
- Building executive-level dashboards and reporting SOC, IR, and vulnerability KPIs (MTTD, MTTR, remediation SLAs, security posture metrics) to senior leadership to support data-driven decision-making.
- Improving team productivity through Jira-based performance dashboards, standardized workflows, clear ownership models, and measurable outcomes.

04/2023 - 02/2024

Mumbai

Lead Cloud Engineer (Promoted)

Cimpress India Private Limited

Promoted to Lead Cloud Engineer after significant contributions to cloud infrastructure

- Successfully migrated 500+ on-premises servers to AWS using Application Migration Service (MGN service), enhancing infrastructure scalability and reliability with zero business disruption.
- Created and controlled AWS EC2 instances, ensuring optimal performance, security, and cost-effectiveness for various applications and workloads.
- Set up and administered AWS Workspaces, providing secure and scalable virtual desktops to support remote work environments.
- Tracked overall AWS infrastructure costs by monitoring usage, optimizing resources, and implementing cost-saving strategies, reducing monthly AWS billing from $60,000 to $40,000.
- Designed and implemented robust AWS cloud solutions, leveraging services such as EC2, S3, FSx, RDS, and AWS Patch Manager to meet business requirements and improve operational efficiency.

EXPERIENCE

07/2021 - 03/2023
Mumbai

Senior Systems Engineer (Promoted)
Cimpress India Private Limited

Contributed to infrastructure engineering as a Senior Systems Engineer

- Supported and oversaw physical server infrastructure, ensuring high availability and performance
- Successfully completed migration of legacy servers to newer platforms, improving system performance and security
- Optimized virtualized environments using VMware and Nutanix platforms
- Conducted server building, installations, configurations, and regular patching
- Performed large-scale P2P, P2V, V2V, Virtual to Cloud migrations
- Managed data stores, created and upgraded templates, and handled virtual machine snapshots and cloning
- Regularly monitored server health, performance, and connectivity issues, responding to alerts proactively
- Troubleshot and resolved issues related to virtual machine performance, network connectivity, and resource allocation

09/2020 - 06/2021
Mumbai

Systems Engineer
Cimpress India Private Limited

Oversaw on-premise environments and cloud infrastructure as Systems Engineer

- Maintained various Microsoft Windows Server operating systems (2003, 2008, 2012, 2016, 2019, 2022), ensuring optimal performance and security.
- Configured and monitored DFS namespaces and replication for efficient file sharing and troubleshooting.
- Administered Active Directory domain controllers, managing replication, user accounts, and group policies.
- Administered and supported Microsoft O365 infrastructure, managing user access and providing end-user support.
- Managed Azure Active Directory, including user management, group policies, and single sign-on (SSO) configuration.
- Administered Microsoft Intune for device management, application deployment, and policy enforcement, ensuring secure and compliant mobile and desktop environments.
- Utilized SolarWinds for server and network performance monitoring, identifying and resolving issues proactively.

10/2019 - 08/2020
Mumbai

Server Engineer
ThinkApps Solutions Pvt. Ltd

Worked as Server & Infrastructure Engineer for a leading Media Client.

- Managed and maintained Windows servers and physical server infrastructure, ensuring high availability and performance
- Administered Microsoft O365, managing user access, email accounts, and providing end-user support
- Developed, enforced, and managed Group Policy Objects (GPOs) to enforce security settings and configurations
- Administered Active Directory, managing user accounts, group policies, and domain controllers
- Managed and optimized VMware environments, ensuring server performance and security

11/2018 - 09/2019
Mumbai

Senior Engineer (Server Management)
Microland Limited

Worked as Senior Engineer in Server Management for a leading Insurance Client

- Administered Active Directory, managing user accounts, group policies, and organizational units
- Managed and monitored domain controllers, ensuring proper replication and security
- Managed and deployed software updates, applications, and patches using System Center Configuration Manager (SCCM)
- Administered Microsoft O365, managing user access, email accounts, and providing end-user support
- Utilized monitoring tools to ensure server and network performance

05/2017 - 04/2018
Mumbai

Desktop Support Engineer (End User Technical Services)
Nityo Infotech Pvt. Ltd

Provided end user support and managed complex projects for a leading Banking & Investment Management Client

- Successfully contributed to the End-of-Service-Life (EOSL) migration project, upgrading 2000+ legacy systems to supported versions
- Provided technical support and troubleshooting for end users, ensuring timely resolution of hardware and software issues
- Managed and maintained desktop infrastructure, including installation, configuration, and upgrades
- Assisted in the administration of Active Directory, Microsoft O365, including email account setup, user access management, and troubleshooting
- Handled IT asset inventory and Vendor Management

CERTIFICATION

CISM

CompTIA Security+

Microsoft Certified: Azure Security Engineer Associate

AWS Certified Solutions Architect - Associate

AWS Certified AI Practitioner

KEY ACHIEVEMENTS

Incident Response Plan
Designed NIST-aligned IR program and DFIR lab, significantly improving incident handling maturity.

AI-Driven SOC Automation
Built an AI-driven SOC triage workflow that cut manual work by ~50%, significantly improving response times

DFIR Lab Setup
Successfully led the establishment of a Digital Forensics & Incident Response lab, enhancing forensic capabilities and incident handling maturity across the organization

Cloud Security Architecture
Led multi-cloud security architecture reviews (AWS, OCI, Azure), driving major attack surface reduction.

Security Leadership
Built and led Information Security program for a global business unit, owning SOC, IR, DFIR, Threat Intelligence, Cloud Security, and GRC.

AWS Migration & Cloud Cost Optimization
Delivered measurable AWS cost savings by optimizing infrastructure and leading the migration of 500+ servers to AWS, achieving ~$20K/month reduction while maintaining high-performance and operational stability.

SKILLS

Information Security & AI Automation

Incident Response | Cyber Forensics | Endpoint & Device Security | SOC Operations | Information Security | Application Security | Cloud Security | Security Architecture | Vulnerability Management | Threat Intelligence | SIEM | EDR | OSINT | Threat Modeling | Network Security | ISO 27001 | NIST | CIS | OWASP | GRC | SSDLC | Security Automation | GitHub Copilot | Python Automation | PowerShell | Cursor AI | Jira | ServiceNow

Infrastructure Engineering (on-premises, virtualized, and hybrid)

AWS | Azure | OCI | VMWare | O365 | SharePoint | Windows Servers | Microsoft Entra | Intune | DNS | DHCP | Active Directory/Azure AD | Identity and Access Management | MDM | MAM

EDUCATION

07/2014 - 05/2017
Mumbai
Bachelor of Commerce
Mumbai University

06/2012 - 05/2014
Mumbai
HSC
Maharashtra State Board

06/2011 - 05/2012
Mumbai
SSC
Maharashtra State Board