Devashish Singh

Information Security Professional

Address Brickfields, KualaLumpur, 50470

Phone 601-133-260976

E-mail devashish.singh12@gmail.com

WWW https://zety.com/profile/devashish-singh/525

LinkedIn linkedin.com/in/devashish-singh-52a050112

Career Synopsis

- Forward-thinking and industrious with diplomatic communication style focused in optimizing coverage to meet security operational demands.
- Agile and adaptable staff leader with stellar work history, motivational approach and upbeat nature.
- Skilled at training and guiding employees.
- Assists senior managers with accomplishing demanding targets by encouraging staff and coordinating resources.
- Hands on experience on Firewalls, Antivirus's, SIEM, Proxy, Email security, Web security, APT Technology, DLP, Multifactor authentication, Vulnerability management, IDS and IPS Solutions, Privacy technologies and Security risk, governance and Compliance.

Skills

Cloud Security — Very Good

Google Cloud platform(GCP) — Very Good

Security Event and incident management - Elasticsearch Logstash Kibana — Excellent

Akamai's and Alibaba WAF(web application firewall) — Excellent

CyberArk IAM(Identity access management) — Excellent

McAfee IPS(Intrusion prevention system) — Excellent

Endpoint protection - Mvision McAfee EPO Trend Micro Deep Security — Excellent

Fireeye - EDR(Endpoint detection and response) — Excellent

Fireeye - EX MX and MAS	Excellent
Tripwire	Excellent
Sophos - Antivirus technology	Excellent
Sophos - Web filtering solution	Excellent
Sophos - Email Security solution	Excellent
Wazuh - HIDS(Host intrusion detection)	Excellent
Penetration testing- Kali Linux	Excellent
DLP - Symantec Forcepoint and Google	Excellent
FluentD - Log collector	Excellent
Firewall - Palo Alto Networks and Checkpoint	Very Good
Google cloud logging Pub sub and Data Flow	Excellent
SIEM technology - Splunk, Chronicles and Elasticsearch	Excellent
Burpsuite - Web application testing	Very Good
Scripting - Python and PowerShell	Good
Proxy - Bluecoat, Zscalar and Microsoft ISA	Excellent
BeyondCorp enterprise - Zero trust model	Very Good
Google Security - Key management reCAPTCHA and Gsuite	Very Good
Google Cloud Armor Cloud IDS	Excellent
RSA Multifactor authentication 2FA	

Good

Varonis DatAdvantage and Datanswers

Very Good

Monitoring - Zabbix Nagios SolarWinds

Very Good

Https://www.cloudskillsboost.google/public_profiles/47074b00-f4a9-4762-b382-1408f08973df

Excellent

Work History

2022-04 - Current

Manager, Information Security Advisor

AirAsia SEA Berhad, Kuala Lumpur, Kuala Lumpur

- Established Cloud and system security posture specifically on Google Cloud platform
- Evaluated and test automations, design, integrations, key management in security domain.
- Developed Yara detection rules in Chronicles and SOAR solutions based on emerging threat and exposures.
- Hands on expertise in BigQuery, Chronicles, Security Command Center, Pub/Sub Integrations, Data Flow, Looker and Elasticsearch to carry out data analysis, classification, forensics and observability.

2020-08 - 2022-04

Information Security, Assistant Manager

AirAsia berhad, Kuala Lumpur, Malaysia

- Working on incident management on endpoint protection, identity access management(IAM), data loss prevention(DLP), SIEM, web application firewall(WAF), Email security solution, web security solution, Advanced threat prevention(ATP), Cloud security solutions, Intrusion detection system(IDS), Intrusion prevention system(IPS), File integrity monitoring(FIM) solution.
- Working on change management on endpoint protection, identity access management(IAM), data loss prevention(DLP), SIEM, web application firewall(WAF), Email security solutions, web security solution, Advanced threat prevention(ATP), Cloud security solutions, Intrusion detection system(IDS), Intrusion prevention system(IPS), File integrity monitoring(FIM) solution.
- Working on problem management on endpoint protection, identity access management(IAM), data loss prevention(DLP), SIEM, web application firewall(WAF), Email security solutions, web security solution, Advanced threat prevention(ATP), Cloud security solutions, Intrusion detection system(IDS), Intrusion prevention system(IPS), File integrity monitoring(FIM) solution.
- Designing security architectures to cover all business assets including high level diagram(HLD) and Low level diagram(LLD).

- Implemented and strengthened SIEM solution and SIEM technology ELK stack and Google cloud Logging - Data collector(Logstash, fluentD, Elasticsearch), Data aggregator, Data ingestion(Google Cloud Pub Sub, Topic, Subscription, Data Flow, Big Query), data analytics and search(Elasticsearch), Data visualization, charts, dashboards(Kibana), SIEM alerts(Elastalert), SIEM events, API integrations, customize plugins, beats shipper(Filebeat, Winlogbeat, Auditbeat, Metricbeat)
- On-boarding and configuring multiple data sources, log sources including but not limited to Network devices, cloud services, Databases, CI/CD pipeline, containers, Docker, Kubernetes, Security devices, middleware, Applications, Software and Operating systems(OS).
- Creating and deploying detection rules based on anomalies, unusual behavior, uncommon processes, heuristics and sandbox results from data collected in Security incident and event management(SIEM) solution.
- Integrating and testing Security incident and event management(SIEM) solution with various threat modules and intelligence services including but not limited to Virus total, abuseurl, abusemalware, malwarebazaar, otx, anomali, anomalithreatstream, recorded future, Cisco Talos intelligence, Snort, Proofpoint emerging threat rules, Socprime.
- Creating and monitoring custom web application firewall(WAF) Alibaba, Crowdstrike and Google cloud armor rules to detect web attacks learned from OWASP top 10, Modsecurity and MITRE attacks tactics, techniques and procedures(TTP).
- Working on McAfee EPO and Mvision endpoint protection solution - covering web protection, safe browsing, antivirus protection, malware protection.
- Monitoring and drafting cloud security best practices rules to classify and respond to Google Cloud platform(GCP) services related vulnerabilities such as IP access, CloudSQL, User roles on Google security command center console.
- Working on GCP security services including but not limited to key management, reCAPTCHA, Identity-aware proxy, we security scanner, risk manager, certificate authority services, BeyondCorp enterprise and cloud armor.
- Created regular expressions, unique identifiers, keywords and custom rules and algorithms for Data loss prevention on Google DLP to prevent data leakage based on data classification, compliance and regulations like GDPR, ISO 27001, PCI-DSS, HIPAA, NIST, COPPA, FISMA, COBIT.
- Working with security testing team to perform POC of reported bugs(On yeswehack) and vulnerabilities from OpenVAS tool.
- Conducted cyber security drill exercise to simulate attack scenario based on phishing protection, spam protection, malware outburst, infections.
- Training and advising stakeholders and fellow colleagues on various security related questions such as security landscape, security best practices, security solutions, security design, security technologies, cloud security etc.
- Creating knowledgebase, documentation, business guidelines, hardening checklists and standard operating procedures(SOP) for security solutions.
- Troubleshooting complex issues related to data leakage, data security, identity theft, data protection, access management and network security.
- Managing team with project tracking, incident handling, guidelines adherence, trainings, task assignation.

- Performing malware analysis, threat hunting and system forensics during incident if needed.

2017-12 - 2020-04

Senior Information Security Engineer

Maybank, Kuala Lumpur, Malaysia

- Delivered successful datacenter migration as subject matter expert of Security solutions for Maybank(A leading bank in Malaysia).
- Built and designed best scalable, available and reliable architecture for security technologies and security solutions such as Intrusion prevention system(IDS), Intrusion detection system(IPS), Privilege Access management(PAS), Identity access management(IAM), Data loss prevention(DLP), Endpoint protection, Compliance check software and data privacy tools, File integrity monitoring, Deep Security, Endpoint detection and Response(EDR), Email Security Analysis and Web Security Analysis.
- Worked on CyberArk as subject matter expert - Deployed and implemented CyberArk components Password vault Web access(PVWA), CyberArk password Manager(CPM), Password vault and privileged session manager(PSM).
- Configured and integrated custom connectors and plugins to support CyberArk CPM password change, password reconcile session capabilities. Example ODBC and McAfee.
- Engaged in day to day CyberArk related operations including but not limited to privilege ID policy management, LDAP integration for authentication, User access control, safe management and disaster recovery(DR) situations, logging, incident management, ID unlocks, grouping, discovery, upgrade etc.
- Configured logging and alerts to work with Splunk, Nagios and Email.
- Delivered Privilege session management(PSM) solution by - conducting POC on multiple data sources, installation and allocation, integration with Vault, customizing connectors SSH and Windows, User access testing(UAT), command control test on SSH.
- Worked on Akamai Web application firewall as Subject Matter expert - Resolved Content delivery network(CDN) related matters on Banking(netbanking/e-banking).
- Delivered On-boarding of web domains as requested by bank.
- Worked on various Akamai products such as Kona Site defender, fast DNS, mPulse, web application protector, Security console.
- Worked on day to day operations including but not limited to Certificate pinning, purge cache, hostname on-boarding, resolve site related errors, create custom WAF rules(OWASP), bot attack prevention, blacklist and whitelist IP during web testing, DNS propagation, site check, troubleshooting connection, resolving user complaints, modifying site parameters.
- Worked on Forcepoint DLP - implementation, testing, upgrade, integration with data classification tools such as Bolden James classifier and Varonis Data Advantage, creating and writing custom rule and regular expressions for data loss detection and prevention, monitoring, uptime assurance and incident management.
- Worked on McAfee Intrusion detection system - Implementation, security detection signature development, custom policies to detect suspicious activities, day to day operations such as health checks, incident management, integrations, connections with network TAP and Firewall.
- Worked on Splunk management - Search Queries, agent deployments, system integration.

- Worked on Tripwire File Integrity Monitoring and compliance check module - configure CIS benchmark based custom compliance check rules, run scheduled quarter scans.
- Represented bank in various audit and regulatory body such as EY external audit, PCIDSS audit, Bank Negara RMIT compliance audit.
- Led teams of up to 6 in developing and implementing security systems, resulting in 30% fewer threats over 1 year.

2016-11 - 2017-11

Security Developer

Inscale, Security Analytics Center, Kuala Lumpur, Malaysia

- Developed and implemented security operations center systems such as Security incident and event management(SIEM) and analytics engines.
- Created runbook, playbooks and technical guides for analysts incident response on various tiers and levels.
- Developed network operations center(NOC) to monitor uptime and handle link failures using Zabbix and Nagios tools.
- Designed network architecture to ensure highly available peer to peer communication for logs forwarding and data collection.
- Configured checkpoint firewall along with IPsec VPN with different different firewall vendors such as Cisco.
- Implemented SSL VPN for user connection to built a stable client service offerings conducted by the team on L1, L2 and L3 levels.
- Helped onboarding new systems by streamlining the change process to the input plugins, output plugins and filter plugins.
- Defined rule based alerts for reliable network and security operations.
- Created spreadsheets using Microsoft Excel for daily, weekly and monthly reporting.
- Led L1 security analyst team in delivery of security operations managed service project, resulting in successful operations.

2016-01 - 2016-11

Firewall engineer

AT&T, Kuala Lumpur, Malaysia

- Project: Royal Dutch Shell.
- Configured and committed firewall rules on client requests on checkpoint firewall R77.10, Fortigate and Zscalar proxy solution.
- Performed pre-health checks and post-health checks including but not limited to cluster health, uptime, peer connection, tail logs, network address translation(NAT), connection limit, system resources, disk usage while implementing rules.
- Performed and reviewed technical security assessments of firewalls and proxy technologies to identify points of vulnerability and non-compliance with established information security standards and recommend mitigation strategies.
- Maintained service level agreement(SLA) to ensure timely delivery of requests to business.
- Validated and verified connection requests from client to identify firewall and proxy to be configured by performing network trace and response analysis.
- Liaised with third parties to respond to firewall related issues.
- Performed network troubleshooting to isolate and diagnose common problems identified in diagnostics, health check results or customer reporting.

2014-06 - 2015-12

Technical specialist

HCL Technologies Ltd, Noida, Uttar Pradesh

- Worked on incident management on Proxies, Web Filters, Email gateway, Antivirus, Data loss prevention (DLP), Two factor authentication, Risk assessment and Security Compliance.
- Worked on problem management on Proxies, Web Filters, Email gateway, Antivirus, Data loss prevention (DLP), Two factor authentication, Risk assessment and Security Compliance
- Worked on Change management on Proxies, Web Filters, Email gateway, Antivirus, Data loss prevention (DLP), Two factor authentication, Risk assessment and Security Compliance.
- Worked on Proxy and Web filter technologies – ISA Proxy, Bluecoat, IronPort and Sophos Web Filter.
- Worked on Firewall Technologies – Palo Alto networks and Cisco ASA(Adaptive Security Appliance)
- Worked on Email Gateway and Email Security solution– Sophos Email gateway
- Worked on Antivirus Technology – Sophos Antivirus
- Worked on DLP Solutions – Control Guard (Host DLP) & Symantec DLP(Email Prevent)
- Worked on FireEye Appliances – EX(Email), NX(Network) and MAS(Malware Analysis)
- Worked on Two factor authentication technology – RSA
- Managed Network devices Cisco ACS with AAA.
- Managed File Integrity, permissions and indexing via Varonis DatAdvantage & DatAnswers
- Performed Penetration testing VAPT on Web Application using Portswigger Burpsuite.
- Documented and created new processes, Standard operating procedures(SOP), Incident handling, technical documentations, technical guides and updating revision controls.
- Managed Security Compliance and perform Internal SOC(security operations center) audits.
- Created checklist to include policy, procedure, standards and guidelines for ISO 27001:20013
- Responsible for Preparing Quarterly and Yearly Audit Schedule, Conducting Internal Audits, Conducting Management Review Meetings, Audit Follow-up, Closure of NCs, Corrective and Preventive Actions, Implementation of Security standards.

2014-06 - 2014-12

Technical Specialist

CMS – Cisco, Bank of America, Noida, Uttar pradesh

- Worked on Internet protocols and Network operations for bank of America.
- Worked on Cisco switches and routers to ensure connection synchronization with Microsoft directory services(AD)
- Registered Domain name system(DNS) records and Dynamic host configuration protocol(DHCP) entries like VitalQIP and Infoblox.
- Administered and worked on Vital QIP and Infoblox related incidents, projects and operations such as upgrade, configuration, reporting and logging.

- Worked on Cisco Any-connect SSL VPN solution.
- Troubleshoot and resolved connectivity issues for business users.
- Improved processes by adding new improvements based on historical issues and reports.

2013-08 - 2014-06

NOC Engineer

FCS Software Solution Ltd, Noida, Uttar Pradesh

- Project: Axalta Coating System.
- Involved in Datacenter migration project.
- Worked closely with Firewall team to design network security architecture.
- Deployed and managed Checkpoint firewall R75.40, R70 and R71 versions GAIA operating system(OS)
- Managed and administered network and server monitoring software's such as SolarWinds and Microsoft system center operations manager SCOM.
- Configured NAT, IPsecVPN, Clustering (Cluster XL) and User based policies by mapping with LDAP and Active Directory.
- Assisted network team on configuration of Virtual LAN, VTP, RSTP, IPsec VPN, SSL VPN.
- Onboarded infrastructure network devices and servers in using protocols such as UDP, TCP, Syslog, SNMP, Netflow.
- Provided technical support in 24x7x365 security and network operations center.
- Planned and oversaw scheduled infrastructure upgrades and integration to respond to organizational demand.
- Handled and escalated critical alerts such as threshold exceed, Disk space overwhelming, Load average, CPU usage, network activity and link failures.
- Identified and categorized equipment issues, responding to calls-for-service to maintain NOC effectiveness.
- Monitored and maintained network and software components according to established guidelines and best practices.
- Provided regular status updates to customers regarding open tickets.

2012-07 - 2013-08

Technical Support Engineer

HCL Technologies Ltd, Noida, Uttar Pradesh

- Served as a technical support engineer to resolve AT&T DSL customers internet connection issues.
- Troubleshoot connections by power cycling routers, modems, light status, reset, performing configuration test, IP test.
- Assessed Customer's query over call and chat acknowledged within service level agreement.
- Defined, tracked, and maintained standard operating procedures for customer experience enhancement.
- Advised best resolution to fix internet connection, email issues and subscription or billing related issues.
- Coordinated with L3 Support and Site Support via Bridge/Conference Call in case of escalation.

Education

2005-05 - 2006-05

Senior School Certificate Examination: Science And Technology

Pratibha Vikas Vidyalaya C.B.S.E - New Delhi

GPA: 83.3

2007-05 - 2008-05

Senior secondary School 12th: Science And Technology

Bhai Parmanand Vidya Mandir C.B.S.E - New Delhi, DL

GPA: 55.4

2008-08 - 2012-12

Bachelors Of technology

Nims University R.T.U - Jaipur, RJ

GPA: 65

Trainings and Certifications

Cisco Certified Network Associate (CCNA)

ACE (Accredited configuration engineer PAN-OS 5.0)

ITIL V.3

Certified Ethical hacking, CEH V8 (ECC97049349115)

CISM - Certified Information Security Manager

CISSP - Certified Information System Security Professional

Languages

English — Excellent

Hindi — Excellent

Affiliations

I DEVASHISH SINGH hereby declare that all the details provided in this resume are correct and true to the best of my knowledge.

Google Cloud Skill badge

https://www.cloudskillsboost.google/public_profiles/47074b00-f4a9-4762-b382-1408f08973df