Jayesh Choudhary,CISSP,CISM

primeash1@gmail.com | linkedin.com/in/jayesh | Github.com/in/Ashdex | FreeIntelhub

Technical Skills

Skills: Python, MITRE ATTACK Framework, MITRE CAR , MITRE D3F3ND, Data loss prevention , Vulnerability Management and Analysis, ,Threat Management, and Endpoint Security Threat Intelligence, Threat Modelling Frameworks, OSINT Security Operations,CTI Network Security Risk Management , CMMI, , ISO270001:2013. Cryptography , Identity and Access Management , Application Security, Privacy Laws and Regulations , Incident Response, Cloud Security , AWS

Security Tools: SIEM ,ArcSight, Symantec, Trellix EPO, Splunk,Proofpoint, ObserveIT, RSAM, JIRA , Wireshark, TheHive , Security Onion,Alienvault, tcpdump, Crowdstrike, AWS , GCP , Azure, Threat Miner,SNOW , Step Security , Vanta , Zeropath , Panther , Elastic

Malware Analysis Tools: STIX , OpenIOC ,MISP , OpenCTI, PEstudio , Regshot , IDAPro , Ghidra , PEID , Resource Hacker , WinDbg , Dependency Walker, Filalyzer , Lord PE , ImpREC , UPX , Maltego , Analyze PE , CAPA , PE Bear , PE Frame , PEV ,EVTVxtract , Unpacker , Unxor , Xortool

Experience

Lead Security Engineer May 2025 - Present

Payatu *Gurugram, HR*

- Built end-to-end threat intelligence automation to aggregate **50+ cybersecurity RSS sources, auto-categorize vendor news (Cisco, Microsoft, Palo Alto, etc.)**, and enable full-text search, reducing manual **triage by 70–80 Percent**
- **Automated IOC enrichment (IPs, domains, hashes)** using AlienVault OTX and VirusTotal with concurrent lookups and scoring to surface high-confidence indicators for faster SOC/IR investigations
- Developed investigation tooling for bulk domain intelligence (Whois/registrar/creation date) and large-scale website snapshot → PDF reporting to support DFIR evidence collection and case documentation.
- Implemented Microsoft Teams → Azure Logic Apps → SharePoint Excel workflows to eliminate manual entry of security advisories and enable near-real-time reporting.
- Led multiple **fintech security engagements** spanning **data protection, threat detection, incident response, and SOC enablement**, acting as primary technical and client-facing lead.
- Developed MSRPC-specific alerts to identify unauthorized access attempts, reducing missed detections by 20 percent
- Delivered **Microsoft Purview DLP** implementation across **400 endpoints and 15+ data sources**, designing **10+ custom Sensitive Information Types (SITs)**, **trainable classifiers**, and **25+ DLP policies**, improving classification accuracy by **40%** and reducing business-impacting violations by **30%**.
- Deployed and integrated **Microsoft Defender, Intune, and Wazuh**, implementing **30+ custom security and compliance policies** and achieving **95% endpoint compliance** with centralized visibility and control.
- Built **30+ MITRE ATT&CK–mapped threat-hunting queries** in **Microsoft Sentinel**, improving detection coverage by **30%** and enabling earlier identification of credential abuse, lateral movement, and persistence techniques.
- Led **incident response and recovery** for active breach scenarios, reducing **mean time to contain (MTTC) by 35%**, identifying systemic control gaps, and driving **15+ prioritized remediation actions**
- Designed and operationalized a **full incident management policy and response program**, including severity models, escalation matrices, and playbooks, improving SOC response readiness and consistency by **40%**.
- Partnered with **IT, Risk, Compliance, Audit, and Senior Management** to deliver **audit-ready assurance artifacts**, enabling **100% closure** of data protection and incident response audit observations.

Cloud Incident Response Sep 2024-May 2025

Coralogix *Gurugram,HR*

- Reduced **MTTD by 40% by engineering** and tuning cloud-native detections across CloudTrail, IAM, and VPC telemetry, improving visibility into privilege escalation and data exfiltration scenarios.
- Decreased **MTTR by 35% by designing automated containment playbooks** that disabled compromised IAM identities and isolated affected workloads within minutes of alert validation.
- Led end-to-end response for high-severity cloud incidents, including IAM compromise and misconfigured storage exposure, preventing potential data impact across production workload
- Identified and remediated critical cloud misconfigurations, enforcing least-privilege IAM and guardrails that improved **overall cloud security posture by 25%**

- Developed and operationalized 30+ cloud detection use cases mapped to MITRE ATTCK (Cloud), reducing **false positives by 30% through contextual enrichmen**t and behavior-based baselining..

Insider Threat Management Officer Sep 2023 – Sep 2024
Bank of America *Gurugram, HR*

- Implemented alerts for identifying data exfiltration through alternate protocols such as DNS/HTTPS Queries
- Created and implemented detection and response alert for Windows Tampering
- Created and implemented detection/response alert for password spray attacks over long duration of time
- Leveraged threat intelligence feeds and analysis to proactively identify potential insider threats, reducing incidents of data exfiltration by 25 percent
- Contributed to insider threat playbooks by incorporating threat intelligence insights, reducing incident response times by 30 percent.
- Applied external and internal threat intelligence to enhance monitoring rules, resulting in a 15 percent reduction in false positives and more accurate identification of malicious insider activities.
- Created and implemented detection/response alerts for Steganography tools
- Identify gaps in present monitoring rules, resulting in **a 15 percent** reduction in false positive alerts
- Continuously monitor internal data sources, such as network logs, user access records, and system activity, to identify any unusual or unauthorized behavior
- Created alert for detecting and monitoring Cryptographic sites
- Created Statement of procedure for stakeholder engagements and control escalations
- Deployed Playbooks and run books for triaging incidents, hence reducing time by **30 percent**

Cyber Security Analyst Sep. 2021 – Aug. 2023
Bank of America *Gurugram, HR*

- Monitored Activity for malicious incidents, managed threats by blocking malicious IP/domains before the user access enabled risk mitigation strategy
- Identified malicious domains with a high risk of data exfiltration and successfully banned access to **over 7,000**users

- Proactively identified and blocked high risk domains that offer high chance of data exfiltration

Graduate Engineer Trainee April 2021 – Aug 2021
CRMNext *Mumbai, MH*

- Implemented and managed CRM systems to streamline customer interactions and improve data accuracy, leading to a 15% increase in customer satisfaction.
- Designed and executed personalized email marketing campaigns using CRM tools, achieving a 20% increase in open rates and engagement.
- Led CRM system upgrades and migrations, ensuring seamless transitions and minimal disruption to business operations

Analyst -Detection And Response April 2019 – Mar 2021

- Designed and tuned EDM- and regex-based DLP detection policies to improve identification of sensitive data patterns.
- Conducted periodic DLP policy reviews and user guidance to improve adherence and reduce policy noise. .
- Refined detection logic to reduce false positives and improve analyst triage efficiency.

Projects

Open Source Threat Intelligence Platform | *Docker,STIX , CTI*June 2022 – Present

- Developed a standalone CTI platform based on OpenCTI and Docker
- Used Docker swarm and Portainer to add Open CTI Stack
- Added TRAEFIK reverse proxy docker and MISP to OpenCTI

Threat Intelligence Dashboard — STIX, TAXII, and MITRE ATT&CK Sept 2022 – Present

- Developed a customized threat intelligence dashboard integrating STIX/TAXII data formats with MITRE ATT&CK framework for real-time threat hunting.
- Implemented automation to ingest and normalize threat feeds from multiple open-source sources, improving detection accuracy by 25 percent
- Deployed threat modeling using the MITRE ATT&CK framework, mapping identified indicators to tactics and techniques, improving response speed.

Homelab for Detection and Monitoring | *Pfsense , Security Onion ,VMware, Splunk* May 2021 – May 2022

- Installed Vmware and configured pfSense firewall for Network Segmentation and Security
- Configured Security Onion as an IDS, Security Monitoring, and Log Management solution and Kali Linux as an attack machine
- Configured a Windows Server as a Domain Controller
- Configured Windows Desktop and Splunk

Certifications :

- ISC2 - Certified Information Systems Security Professional (CISSP)
- ISACA Certified Information Security Manager (CISM)
- ISACA Certified Information Systems Auditor (CISA)
- CompTIA Security+
- CompTIA Pentest+
- CompTIA CySA+
- CompTIA CASP+
- CyberSec First Responder - CFR-410
- Google IT Professional Certificate
- Microsoft SC-300
- Microsoft SC-900
- CSA CCSK V.4
- CSA CCSK V.5
- Microsoft SC-200
- Microsoft AZ-500
- Microsoft SC-100