**CURRICULUM VITAE**

Himanshu Chaurishiya

A-21 Shri Ram Colony, Borkhera Kota (Rajasthan)

Email: himanshu.chaurishiya@gmail.com

Mobile No: +917875503835

LinkedIn: https://www.linkedin.com/in/himanshu-chaurishiya-🇮🇳-965b9a126



**SYNOPSIS**

To seek a challenging position in the domain of Information security where I could utilize my years of experience and knowledge for solving problems in a creative manner.

**PROFILE SUMMARY**

* CEH Certified and holds other certification ie .Vectra,API Security
* Actively worked with top management to set up a automation environment within SOC using API and other TIP, soar tools.
* Managing 4 members of team currently and defining the incident handling procedure and process.
* Develop reporting and KPI for management to show achievements and value of SOC.
* Responsible for training the team on incident monitoring, Incident analysis and malware analysis.
* Analysis of correlated security incidents, to identify malware infections, web attacks, suspicious behavior attack, scanning activity etc and suggest remediation steps.
* Working experience of Security Information and Event Management (SIEM) solutions.
* Scripting or programming experience.
* 6 + Years of Experience as Malware Analyst & Secure internal customers
* Awarded as 1 Bright Spark, 3 best@INDEC,1 Innovation Jury Award and also Promoted within a six-month timeframe for exceeding goals and supporting company culture
* Working Knowledge of Ticketing Software i.e., JIRA, Resilient and Service Now
* Hands on experience on additional products i.e., Proofpoint Tap, McAfee EPO, GroupIB, Vectra, crowdstrike, carbon black with API knowledge

**EXPERIENCE**

**Saint-Gobain, Mumbai**

**SOC (Team Lead-Cyber Threat Intelligence) | January 2022—Present**

* Handling CTI, Vulnerability Assessment and Sandboxing services.
* Demonstrable knowledge of attack vectors, threat tactics, attacker techniques, and the Cyber Kill chain.
* Use of news aggregator to get the insights about latest vulnerability, breaches, malware campaigns, Indicator of compromise and Security Highlights
* Threat Intelligence products and administrator
* Perform daily review of bulletins, alerts, incident reporting documents and tracking excels.
* Working Knowledge of TAXII and STIX.
* Setting up Threat Intelligence Platform and its integration. Developed a custom responders and analyzers.
* People Management based on projects and other Administration work.
* Bring the productivity in the team using automation skills also with low-code technologies ie MS flow and incoming webhooks.

**Senior Security Engineer(Team Lead) | January 2020—January 2022**

**Threat Analyst | June 2019—December 2019**

* Experience working with Security Information and Event Management (SIEM) solutions.
* Develop custom tools for cybersecurity departments
* Perform cyber threat intelligence operations including intelligence collection (IOCs), tracking threat actors, identifying and tracking malicious infrastructure.
* Develop reporting and KPI for management to show achievements and value of SOC.
* Experience with automated incident response tools (Sysmon, Carbon Black, Vectra AI).
* Experience reviewing and assessing logs for anomalous activity indicating the presence of a threat.
* Demonstrable knowledge of attack vectors, threat tactics, attacker techniques, and the Cyber Kill Chain.
* Scripting or programming (Shell scripting, PowerShell,Python)
* Hands on experience on additional products ie .Proofpoint Tap,McAfee EPO,GroupIB.
* Managing Team of two different project as role of Team Lead

**SOPHOS,Ahmedabad**

**Threat Researcher**

**Jan,2017-June,2019**

## Dynamic and Static Analysis of Windows Malware Samples in Controlled Environment

## Working knowledge of file formats such as PE,PDF,NON-PE,Doc etc.

## Experience with memory dumps. Knowledge of windows Internals & API.

## Provides incident response support, Identifying & prioritizing potential threats.

## Supports computer forensics & malware analysis.

## Passion for reverse engg & taking on the bad guys.

## Solve customer and internal query.

**Max Secure Software,Pune**

**Software Developer(Malware Analyst)**

**Oct,2015-Jan,2017**

## Develop Android Apps

## Dynamic and Static Analysis of Android/Windows Malware Samples in Controlled Environment.

## Knowledge of networking protocols such as TCP/IP, DNS, SMTP etc.

## Creating signatures for detecting malware through static and dynamic analysis.

## Analyzing new malwares and studying its behaviors for classification.

## Making Reports describing the threat.

## Help Android Developers by providing code from APKs.

## Performing assigned tasks with diligence, producing work of good quality and being a reliable work.

## Create yara rules to detect similar behaviour of malware sample.

## Reading blogs of various security experts.

**Skills**

## Usage of IDA Pro,OllyDbg,ILSpy,JD-GUI ,Wireshark etc.

## Knowledge of networking protocols: TCP/IP, HTTP/HTTP s.

## Basic knowledge of programming language.

## Expert in usage of security tools ie microsoft network tools,sysinternal tools etc.

## Excellent communication skills and ability to adapt to the audience.

## Be able to work independently on tasks as well as work well within a team environment.

**Education**

* Currently pursuing the M.Tech in Software Engineering from BITS Pilani
* CDAC:PG-Diploma in Wireless and Mobile Computing,Pune(2015)
* B.Tech:Computer Science(2014)

**Articles Published**

PDF Analysis with NTLM Hashes Theft analysis

Link :<https://www.linkedin.com/feed/update/urn:li:activity:6529518487759613952>

# MageCart-10k+ --Part1

Link:<https://www.linkedin.com/pulse/magecart-10k-part1-himanshu-chaurishiya->

Malware Analysis:

Link:<https://www.linkedin.com/pulse/malware-analysis-himanshu-chaurishiya--1d/>

**Updated date: 18th January 2022**