

# Apurv Singh Gautam

apurvsinghgautam@gmail.com

apurvsinghgautam.me

## PROFESSIONAL SUMMARY

---

I am a Cybersecurity researcher with 5 years of progressive experience seeking a Threat Intelligence Analyst role. I perform threat hunting on the surface web and dark web and analyze and produce threat intelligence. I enjoy reading threat reports, white papers, and blogs. I have been attending and speaking at many conferences, including SANS, DEFCON RTV, Diana Initiative, and many more. I love being involved and contributing to the security community

## EXPERIENCE

---

- **Georgia Institute of Technology** Atlanta, US  
Head Teaching Assistant Aug 2019 - Present
  - **Course:** CS 4235/6035 Intro to Information Security, CS 6250-001 Computer Networks
  - Managing 4 TAs and 160 students
  - Creating weekly quiz questions for different security topics
  - Grading assignments, quizzes, projects and exams
- **International Computer Science Institute, UC Berkeley** Berkeley, US  
Security Research Intern May 2020 - Jul 2020
  - **Area:** Threat Intelligence - Creating threat intelligence metrics
  - Performed deep dive analysis of malicious data from 4-5 dark web forums/markets
  - Analyzed the large unstructured data using advanced NLP algorithms (LDA, CatE)
  - Created 6 high-level threat intelligence metrics for the analyzed data
- **Volon Cyber Security Pvt. Ltd.** Pune, India  
Security Research Intern May 2018 - May 2019
  - **Area:** Threat Intel/Hunting - Obtaining Intelligence from surface/dark web forums
  - Performed advanced open source intelligence (OSINT) on surface web and dark web sites
  - Performed threat landscape analysis on dark web forums and markets
  - Created an advanced automated scraping tool to scrape data using Python Scrapy
  - Scraped unstructured data of about 10-20 dark web forums and markets into elasticsearch
  - Performed human intelligence (HUMINT) on the dark web forums and marketplaces
  - Conducting various threat investigations and preparing a finished report in the form of TTPs

## SECURITY COMMUNITY INVOLVEMENT

---

- **BSides Toronto '20, BSides DFW '20, GrayHat Blue Team Village '20:** CFP Accepted
- **SANS Cyber Defense Forum '20, RootCon '20, BSides Singapore '20, The Diana Initiative '20, DEFCON 28 Red Team Village '20:** Delivered a talk on Automating Threat Hunting on the Dark Web and other nitty-gritty things [\[Video\]](#)[\[Video\]](#)[\[Video\]](#)
- **GRIMMCon 0x2 '20:** Delivered a talk on Threat Hunting on the Dark Web [\[Video\]](#)
- **CTI League:** Volunteering as a Darknet researcher, creating crawlers and scrapers to scrape from the darknet for monitoring healthcare threats
- **Cybrary:** Volunteering as a Senior Teaching Assistant, managing security-fundamentals channel, creating materials for several security courses, including Intro to Threat Intelligence, Insider Threats, Intro to TOR, and many more
- **StationX:** Volunteering as a Teaching Assistant, moderating the discourse, engaging with the community, and solving course-related doubts
- **Cybercademy:** Volunteering as a Community Challenger, managing the discord and creating security challenges for students

- **SIT, Pune:** Presented two seminars on starting in cybersecurity for high-school students and cybersecurity certification batch students and conducted NS3(Network Simulator), Git, and Virtualization Buddy Session for third-year Computer Science and Information Technology students
- **MITCOE, Pune:** Conducted a Cyber Privacy Seminar on behalf of the Logout - Privacy Seminar
- **Null, Pune:** Delivered several talks including Introduction to VAPT, Bitcoin Forensics, and OSINT
- **TAIS, Varanasi:** Conveyed a two-day workshop on Cyber Security Awareness

## SKILLS

---

- **Programming:** Proficient in Python, Java, and Bash. Fundamentals of C, C++, PHP, JavaScript
- **Security:** Threat Intelligence, Threat Hunting, OSINT, HUMINT, Security Analysis
- **Miscellaneous:** Elastic Stack, MITRE ATT&CK, NLP

## OPEN SOURCE CONTRIBUTIONS

---

- **OnionIngestor:** OnionIngestor is based on ThreatIngestor tool structure to enable modular and extendable access for Cyber Threat Intelligence teams so that they can monitor and collect information on hidden sites over tor network. [\[Project\]](#)
  - Created 5 sources to extract .onion domains with 8 sources in total
  - Utilizes 4 operators including html source, screenshot, onionscan, and yara
  - Stores analyzed data into Elastic stack
  - Produces daily reports and sends the notification to Kibana and Telegram
- **Free CyberSecurity Professional Development Resources:** An awesome list of resources for training, conferences, speaking, labs, reading, etc that are free all the time that cybersecurity professionals with downtime can take advantage of to improve their skills and marketability to come out on the other side ready to rock. [\[Project\]](#)
  - Contains upcoming conferences and instructor-led webinars/trainings
  - Consists of security podcasts, YouTube channels, and news websites

## RELEVANT PROJECTS/RESEARCH WORK

---

- **ForumScrapy:** Web Scraping application built on Flask that scrapes forum posts from the Bitshacking hack forum [\[Project\]](#)
  - Created an automated scraping tool using Python
  - Scrapes forum data from Bitshacking hack forum
  - Utilizes several socks proxy chains to scrape the data
  - Utilizes Elastic Stack to store the data and visualize it
  - Created dashboard using Flask to view and interact with data with search capabilities
- **PastebinScrapy:** Threat Hunting tool built on Flask that scrapes IOCs, including IP addresses, hashes, and emails from Pastebin's latest pastes [\[Project\]](#)
  - Created an automated scraping tool using Python
  - Scrapes latest pastes from Pastebin using Pastebin's Scraping API
  - Collects IOCs like IP addresses, hashes, emails from the latest pastes using regex
  - Utilizes Elastic Stack to store the data and visualize it
  - Created dashboard using Flask to view and interact with data with search capabilities
- **Applying Diamond Model on WannaCry Ransomware Incident:** This blog maps WannaCry ransomware incident to the Diamond model that includes all components of the model [\[Blog Post\]](#)
  - Performed case analysis with diamond model including victim, infrastructure, capability, adversary
  - Discussed extended diamond model that includes social-political and technological meta feature
  - Performed case analysis with policy impact

## EDUCATION

---

- **Georgia Institute of Technology** Atlanta, US  
Master of Science in Cybersecurity (M.S.); GPA: 3.75 2019 - Expected May 2021
- **Symbiosis Institute of Technology** Pune, India  
Bachelor of Technology in Information Tehcnology (B.TECH); CGPA: 8.63 2015 - 2019