# SWAPNIL GOUD TADKAL

📬 8980 Red Bud Street, Parker, CO – 80134 | ✆

📧: [swapnil.tadkal@outlook.com](mailto:swapnil.tadkal@outlook.com) : [www.linkedin.com/in/swapnil-goud-tadkal](http://www.linkedin.com/in/swapnil-goud-tadkal)

## Profile Summary

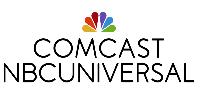
Currently working as a Staff Security Incident Response Analyst at GoTo by leveraging Incident Response procedures, SIEM skills and knowledge of computer forensics to provide better security for GoTo and its users. Also I taught Computer Forensics I at Colorado Technological University as an Adjunct Instructor. I have Masters in Computer Forensics from George Mason University.

Have proven my skills in Incident response, Detection Engineering, Computer Forensics, Ethical Hacking, Log Analysis, Event Monitoring, Network Security (IPS/IDS) and Threat Management through different SIEM tools.

## Experience

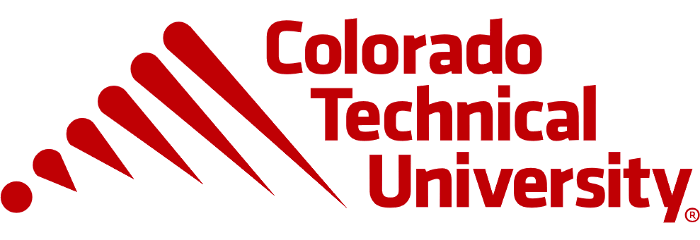
### Staff Security Incident Response Analyst at GoTo Nov 2020 to till date

* Identify security issues and risks associated with security events and be a major stakeholder in the incident response process.
* Work as Liaison for Splunk ES to manage, Develop and fine-tune.
* Design, build and manage (“own”) the detection engineering program for LogMeIn; both with on-prem and cloud (AWS and Azure) infrastructures.
* Optimize and customize security-monitoring tools in order to improve detection
* Understanding of the tactics, techniques and procedures of advanced attackers; in order to hunt for signs of Advanced Persistent Threat (APT) activities
* Utilize security models and frameworks for documenting and tracking purposes, (e.g., MITRE ATT&CK framework, Cyber Kill Chain (CKC) framework)
* Develop comprehensive and accurate reports and presentations for both technical and executive audiences
* Train, coach and mentor more junior Security Analysts on the CSIRT
* Assist in identifying, evaluating and providing feedback for potential talent to join the CSIRT.
* Collaborated with cross-functional teams to ensure timely delivery of projects.
* Provided training sessions on new technologies and tools designed to enhance productivity and efficiency.
* Engage, invoke, and oversee 3rd party breach and forensic retainer service providers as needed.
* Collaborate with SOC analysts as a Incident Coordinator to develop and facilitate threat-based IR tabletops and Simulation Scenarios, raising awareness and identifying IR process improvement opportunities.



### Security Incident Response Engineer (SIRT) at Comcast Cable Corporation, Denver, Colorado.

### March 2018 to Nov 2020

* Worked on POC for new SIEM consisting of Splunk, LogRythm and Qradar cloud versions to update the SIEM in Comcast.
* Investigate opportunities to update security system capabilities or perform policy updates based upon system performance reports and observed incidents or threats.
* Participate in the post-mortem investigation of catastrophic network security incidents and prepare security incident reports documenting the findings.
* Assist with security compliance audits to verify completeness of security required configurations and verify system hardening.
* Ensure timely proactive identification and reporting of security gaps and vulnerabilities to the critical business information, systems and network infrastructure.
* Develop, execute, and maintain security incident management procedures for large ISP network and systems.
* Develop, execute and maintain security system fault management support procedures for assigned systems.
* Check Security policies assigned for Cloud accounts in **AWS** or **Azure**.
* Automate procedure with the help of **Demisto** by creating Playbooks for efficiency and speediness in the process of investigation.
* Perform configuration updates, such as modifying configurations, signature definitions or implementing new policies on various security tools like **Carbon Black, Symantec, ArcSight, FireEye,** and **Arbor** etc...
* Coordinated with vendors regarding maintenance of existing security products and services
* Evaluated new technologies related to information security and recommended changes accordingly.

### Adjunct Instructor at Colorado Technological University, Denver, Colorado.

### June 2018 to Oct 2018

* Teach **Computer Forensics I** to undergraduate students.
* Help them to understand basics of Computer Forensics and introduces the student to the field of computer forensics.
* The hands-on intensive course examines procedures for investigating computer and cyber-crime and concepts for collecting, analyzing, recovering and preserving forensic evidence.
* Encouraged students to develop an enthusiasm for learning by proving a stimulating educational atmosphere

### Cyber Security Specialist at Hill Technologies, District of Columbia (DC). July 2017 to March 2018

* Manage security incidents from different agencies present.
* Conduct security tool/application (**McAfee Nitro**) tuning to develop/adjust rules and analyst response procedures and reduce false-positives from alerting.
* Work with **Palo Alto**, **Check Point**, **Infoblox**, **Sourcefire**, and **McAfee EPO** in collaboration with **Nitro ESM** for better investigative results.
* Recognize, create and ingest Indicators of Compromise (IOC’s) for attacker tools, tactics, and procedures.
* Provide technical analytical guidance to, and quality-proofing of tier 1 analysts analytical advisories and assessments prior to release from SOC.
* Coordinate with and provide expert technical support to enterprise-wide technicians and staff to resolve confirmed incidents.
* ****Provide in-depth cybersecurity analysis, and trending of log, event data, and alerts from diverse network devices and applications within the enterprise to identify and troubleshoot specific cybersecurity incidents and make sound recommendations that enable expeditious remediation.

### Precollege Cybersecurity Instructor

### George Mason University, Fairfax, Virginia Oct 2016 to May 2017

* Teaching Precollege Cybersecurity Level 3 (CompTIA Security +), Level 4, 5 (CEH), Level 6, 7 (C|HFI) programs.
* The hands-on intensive Precollege Cybersecurity program prepares middle and high school students to apply technical skills in cybersecurity careers.

### Graduate Research Assistant at School of Business, George Mason University May 2016 to Dec 2016

* Worked on Python Scripts to collect data from Google and validate it accordingly.

### Graduate Teaching Assistant at George Mason University. September 2016 to Dec 2016

* Grade Assignments and help students to clear their doubts in CYSE 330 (Intro to Network Security) and CYSE 425 (Secure RF Communications) courses.

### Advisory Analyst at Deloitte & Touché Assurance & Enterprise Risk Services India Private https://upload.wikimedia.org/wikipedia/commons/thumb/5/56/Deloitte.svg/1000px-Deloitte.svg.png

### August 2014 to December 2015

#### SIEM – Managed Security Services/Cyber Intelligence Center (Deloitte-CIC)

* Developed client specific Threat Use Cases (TUCs) leveraging ArcSight tool and tuning of the TUCs, Hunt Analysis transforming them to actionable cases, assisted in drafting of the procedural documents and run books.
* Monitoring and L1/L2 activities, investigation of malicious events and incidents, Creation of cases based in initial investigation and suspected malicious activity, DDoS identification and notification.
* Spot Award for adding value to the client engagement and recognized for “Event analysis and recommendations to Canadian team to fine tune the SIEM use cases”.
* Worked on several **S**ecurity **I**ncident and **E**vent **M**anagement (SIEM) tools like HP **ArcSight**,IBM **QRadar**, McAfee **Nitro Security**, **Splunk**

#### Vulnerability Assessment and Penetration Testing

* Trained on Cyber Security and Cyber Operations Management, Information Security Standards, Web applications and Network Security, Mobile Security Principles. Gained hands-on experience working with Network Security assessment tools and operations and had a simulation exposure on performing vulnerability assessments on Networks and Web Applications.

#### Security Information and Event Management (SIEM) (Internal Training)

* Initial setup of SIEM, deployment and implementation of SIEM solution leveraging HP ArcSight, Integration of new and existing devices with the implemented SIEM solution, Development of use cases and generation of reports for the same.

#### Cyber Threat Intelligence Services/Cyber Threat Profiling

* Performed Cyber Threat Profiling for a major Global Provider of Financial Services Technology Company, Internet foot printing of client, Identification of potential vulnerabilities, Organization threat modelling, Potential recommendations.

#### Data Loss Prevention

* Worked on projects related to Data Loss Prevention using **RSA DLP** tool protecting their important data from leaving the firm either through Email, External memory drives, Cloud services

### Digital Forensics Investigator Intern in Hyderabad Cyber Lab, Crime Investigation Department, Hyderabad. November 2013 to June 2014

* Applied advanced techniques such as forensic analysis to support investigations.
* Assisted in several cyber cases as a **Digital Forensic Investigator**
* Provided trainings in the field of Cyber-crime investigation and Digital Forensics to several Police officials in Andhra Pradesh Police Academy (APPA) and Crime Investigation Department (CID).

## Education

Masters in computer Forensics | Jan 2016- May 2017 | **George Mason University**, Fairfax, VA.

* Secured 3.73 out of 4.00 GPA

|  |  |
| --- | --- |
| **CFRS 500:** Intro to Technology of Forensic Value | **CFRS 660:** Network Forensics |
| **CFRS 664:** Incident Response Forensics | **CFRS 763:** Registry Forensics |
| **CFRS 762:** Mobile Device Forensics | **CFRS 771:** Digital Forensics Profiling |
| **CFRS 760:**Legal and Ethical Issues in Computer Forensics | **CFRS 661:** Digital Media Forensics |
| **CFRS 790:** Advanced Computer Forensics | **CFRS 780:** Memory Forensics |

### Bachelor of Technology in Computer Science Engineering | 2010 – 2014 | Jawaharlal Nehru Technological University, Hyderabad, India.

* Secured 3.3 out of 4.00 GPA

## Certification & Training:

* **EC Council** Certified Computer Hacking Forensic Investigator (**C|HFI**)
* **SANS SEC401**: Security Essentials – **GSEC**
* **Splunk** Fundamentals Part 1
* **Splunk** Fundamentals Part 2
* **Splunk** Advanced Searching and Reporting
* **SANS MGT525:** IT Project Management, Effective Communication, and PMP® Exam Prep
* **SANS SEC504:** Hacker Tools, Techniques, Exploits, and Incident Handling
* **SANS SEC573:** Automating Information Security with Python - **GPYC**

## Skills & Abilities

### Leadership

* Lead a team of 60+ members (Tier 1 & Tier 2) in Comcast.
* Lead the team of 10+ people at OCTO DC Govt.
* Acted as one of the head committee in Indian Graduate Student Association (IGSA) at George Mason Univ.
* Acted as Class Representative during bachelors.

### Team player

* Work with a team of 100+ people (Different locations in US and India) and coordinate with all other teams in Comcast Cable Corporation.
* Worked as a Volunteer for OSDFCon 2016.
* As a part of Head committee for IGSA, made sure we help Indian students (New admits and Old) have an easy and wonderful experience in USA.
* Was part of team of 50 members in SOC, providing security services to the clients
* Trainer - New Hire Orientation (NHO-2014). Trained new hires on SIEM technologies, SOC and CIC operations and activities.

### Management

* Manage teams present in US (different locations) and India working 24/7.
* Managed schedules for complete team of 50 members to provide 365\*24\*7 services to the clients.
* Acted as a lead and provided several daily/weekly reports to the clients on behalf of management.

### Technical

* **Operating Systems**: Linux (Ubuntu, DEFT, Kali, Bugtraq), Windows (XP, 7, 8, 10), Macintosh
* **SIEM Tools**: HP ArcSight, IBM QRadar, McAfee Nitro, Splunk, LogRythm
* **Scripting Tools:** Python, Shell script**,** PowerShell
* **DLP Solutions**: RSA DLP, Symantec Enforcer
* **Security Assessment tools**: Nmap, Wireshark, Nessus, StealthWatch
* **Reporting tools:** Demisto, Archer, BMC Footprints, BMC Remedy, Atlassian JIRA, OTRS, RT
* **Forensic tools:** Magnet Axiom, Autopsy, FTK, Encase, Volatility, Oxygen
* **Security Tools:** Check Point Smart view, InfoBlox, Arbor Network APS, McAfee EPO, Palo Alto, Sourcefire, Symantec, NCircle, Bluecoat, TruStar, Demisto, MITRE Attack
* **Cloud Networks:** Amazon Web Services (AWS), Azure