Chaitanya Krishna Anantharapu
Contact: (+91) 801 927 4215| **Email:** chaitanyapentest@gmail.com
LinkedIn: https://in.linkedin.com/in/chaitanyakrishnaa
GitHub: https://github.com/chaitanyakrishna/

INFORMATION SECURITY CONSULTANT

Experienced IT professional with over 10+ years of experience in the design, development, and management of Information security services for both private and public sector

---

Cyber Threat Intelligence | Incidence Response |Security Assessments | OSINT | SOC Operations |Training & Development

- ☑ Significant experience and expertise in all areas of information security and cyber threat intelligence including program design and implementation.
- ☑ Demonstrated success in guiding the implementation of leading-edge technology solutions while balancing security initiatives with risks, business operations, and innovations.
- ☑ Developed course curriculum for beginners on specialist areas including Penetration Testing with Metasploit.
- ☑ Ability to develop and present reports with a good mix of space & time complexity. Excels in undertaking Binary Analysis and is capable of presenting conceptual data to clients.
- ☑ Multilingual communicator with an innate ability to work with and train cross-functional and multi-disciplinary teams; communicates and understands the voice of global clients from diverse nationalities.

TECHNICAL SKILLS

- ☑ Incident Response, Cyber Threat Intelligence, Open Source Intelligence
- ☑ Strategic, Operational, and Tactical cyber threat intelligence
- ☑ Open source intelligence and Threat Actor campaigns
- ☑ Cyber Threat Intelligence Analysis, attribution, collecting and storing data sets
- ☑ Triage and respond to potential threats
- ☑ MITRE AAT&CK Framework for Enterprise
- ☑ Application Vulnerability Assessment and Penetration Testing of Web Applications and Networks
- ☑ Realtime Attack Surface Analysis & Vendor Risk Management
- ☑ Experience performing application security testing and presenting mitigation recommendations to IT and Business
- ☑ Demonstrating Web Application Vulnerabilities of OWASP top 10 such as Cross-Site Scripting (XSS) and SQL Injection, Broken Link Authentication, Session Hijacking, and Cross-site request forgery
- ☑ VA/NPT/APT Process and tools such as Acunetix/App Scan/Web Inspect/Nessus/NetSparker
- ☑ Penetration Testing – Network, Host, Web Applications
- ☑ Black Box and White Box Penetration Testing (i.e. Internal/External PT)
- ☑ Good knowledge on different penetration testing methodologies
- ☑ Foot printing, Different types of Scanning, Network Reconnaissance
- ☑ Browser, Local and remote exploits
- ☑ Penetration frameworks like METASPLOIT for Compiling and Changing payloads of various Exploits
- ☑ Good knowledge on Python, PowerShell scripting for performing automation jobs
- ☑ Sniffers like Tcpdump, Wireshark, Cain & Abel and can do analysis, extract data from CAP and PCAP
- ☑ Familiar with different security tools used for Network Scanning, Web application vulnerability assessment, IDS and Wireless Security

CAREER REVIEW

Cybersecurity Specialist – Threat Intelligence ▸ Prime Medical Technologies **SEP 2020 – TILL DATE**

- ☑ **Key Roles & Responsibilities:** Led execution of Cyber Threat Intelligence Team for Prime Healthcare group of hospitals, established Threat Intelligence automation process.

- ☑ **Key Deliverables:**
- ☑ Provide analytic support in the areas of dependency and interdependency analysis, analysis of cascading impacts, and cyber/physical risks to critical infrastructure.
- ☑ Provide proactive and reactive end-to-end threat intelligence services to help protect external facing and internal based computing assets, data, and global clients.
- ☑ Support key, high-profile cyber security-related activities pertaining to the healthcare industry and IOT product security, including support for the Primehealthcare group incident response program.
- ☑ Provide actionable intelligence for enterprise risk reduction and remediation by partnering with security teams in identifying and driving risk remediation approaches to current and emerging threats.
- ☑ Developed complex analytical approaches to problems and situations for which data is incomplete, controversial, or no precedent exists.
- ☑ Develop, lead, and brief senior leadership regarding critical best practices/capabilities pertaining to cyber issues on a proactive basis.
- ☑ Develop innovative approaches to analyse and validate analytical conclusions.
- ☑ Maintain and update databases, systems, and mechanisms for sharing relevant intelligence information to support ongoing and projected projects.
- ☑ Develop Threat reporting and techniques, tactics, and procedures (TTP's)
- ☑ Deliver Strategic, Operational, and Tactical cyber threat intelligence.
- ☑ Provide Summarised complex information security concepts and ongoing threat events for management Consumption.
- ☑ Designed and Developed automation scripts for Cyber threat intelligence team activities to reduce the delta time in achieving security orchestration process.
- ☑ Deliver brown bag sessions for security teams for improvising security posture and deliver training according to the team's requirement.
- ☑ Develop standard operating procedures for the team requirements and processes.

IT Security Specialist ▸ Agility E-Services **November 2018 – May 2020**

- ☑ **Key Roles & Responsibilities:** Led the execution of security initiatives by deploying, configuring and supporting security technologies, carrying out security assessments, identifying client's security requirements, and ensuring that they are implemented. Provide assurance by collecting proof that implemented security controls are operating as designed.
- ☑ Conducting technical and forensic investigations into matters raised through alerts, intelligence, testing activities and end user reports that lead to a coordinated effort to effectively contain, mitigate, and remediate active and potential attacks.
- ☑ **Key Deliverables:**
- ☑ Performing the forensic services for the collection, processing, preservation, analysis, and presentation of evidence in support of vulnerability mitigation and information security incident investigations.
- ☑ Undertook MSSP's assistance to lead the investigation by using suite of tools like End Point Detection and Response – CarbonBlack Response, SIEM – SecureWorks, Threat Detection and Response – RedCloak and Endpoint Security by using Cylance.
- ☑ Conduct iterative threat hunting to proactively search for and isolate advanced threats that evade existing security solutions.
- ☑ Collaboration with global teams in the production and maintenance of efficient and effective incident response playbooks.
- ☑ Supporting the Identification, development and implementation of new detections use cases.
- ☑ Developing and defining detailed processes and procedures to manage the response to cyber security events.
- ☑ Directly contributing to the continued technical enhancement of the security platforms.
- ☑ Supporting the continued evolution of incident response and forensic capabilities and processes, including automation and orchestration.
- ☑ Training and developing other members of the Incident Management and Response team as well as other members of the Global Cybersecurity Operations function.
- ☑ Perform independent analysis of complex problems and distill relevant findings and root causes.
- ☑ Leverage threat intelligence to search for the presence of Indicators of Compromise (IOCs) across the enterprise.
- ☑ Process, analyse, and develop metrics reporting capacity, including automation, visualization and analytics to accurately capture types of threats and attacks and their sources and the actions taken by the IT Security team in response.
- ☑ Monitor and analyse security events collected by the SIEM, and identify trends, attacks, and potential threats.

Senior Analyst – Cyber Threat Intelligence ▸ Deloitte USI **May 2017 – Oct 2018**

- ☑ **Key Roles & Responsibilities:** Provide customized Threat Intelligence to Deloitte Member Firms of various GEO regions customers.
- ☑ Develop Cyber Threat Intelligence Requirements, Collect Cyber Threat Information, Provide Strategic Cyber Threat Intelligence, Analysing and Disseminating Cyber Threat Intelligence.
- ☑ **Key Deliverables:**
- ☑ Provide analytic support in the areas of dependency and interdependency analysis, analysis of cascading impacts, and cyber/physical risks to critical infrastructure.
- ☑ Provide proactive and reactive end-to-end threat intelligence services to help protect external facing and internal based computing assets, data, and global clients.
- ☑ Support key, high profile cyber security related activities and projects, including support the global client's incident management program.
- ☑ Provide actionable intelligence for enterprise risk reduction and remediation by partnering with key groups in identifying and driving risk remediation approaches to current and emerging threats.
- ☑ Develop complex analytical approaches to problems and situations for which data is incomplete, controversial, or no precedent exists.
- ☑ Develop, lead and brief senior leadership regarding critical best practices/capabilities pertaining to cyber issues.
- ☑ Develop innovative approaches to analyse and validate analytical conclusions.
- ☑ Maintain and update databases, systems, and mechanisms for sharing relevant intelligence information to support ongoing and projected projects.
- ☑ Develop Threat reporting and techniques, tactics, and procedures (TTP's)
- ☑ Provide Summarised complex information security concepts and ongoing threat events for management Consumption.

Security Analyst L3 ▸ EIQ Networks India R & D Private Limited **Feb 2016 – May 2017**

Key Deliverables:

- ☑ **Key Roles & Responsibilities:** Responsible for delivering SOC services for the global customers which include Vulnerability Assessments, Incident analysis. Creating and reporting security incidents to prevent additional loss and offer mitigation techniques to minimize attack vectors.
- ☑ Handling large enterprise customers for implementation of security services Creating security reports and ensure compliance with security advisory and best practices recommendation.
- ☑ **Key Deliverables**: Performing regular security assessments. Actively investigating the latest security vulnerabilities, advisories, incidents, and penetration techniques and notifying clients when appropriate. Creating and responding to security incidents to prevent additional loss and suggesting mitigation techniques. Responsible for SOC Implementation, Onboarding, Baselining, Environmental Analysis, Health. Check, Alerts Fine Tuning, Device Integration.

Enterprise Risk Services Consultant (RETAINER)▸ Deloitte Touche Tohmatsu India LLP, Delhi Jul 2015 to Jan 2016

Key Deliverables:

- ☑ **Key Roles & Responsibilities:** Work closely with members of the security team in managing corporate and large divisional systems development projects for Government of Delhi, Karnataka and Jharkhand.
- ☑ Offer mitigation techniques for the different types of existing vulnerabilities and exploits. Explain the magnitude of potential business and operational impacts of successful attacks.
- ☑ **Key Deliverables**: Led the execution of security initiatives by deploying, configuring and supporting security technologies, carrying out security assessments, identifying client's security requirements, and ensuring that they are implemented. Provide assurance by collecting proof that implemented security controls are operating as designed. Hold overall accountability of creating and developing security policies and procedures for Government of Delhi.

Independent Information Security Consultant **Oct 2012 to Jul 2015**

Key Deliverables:

- ☑ **Key Roles & Responsibilities:** Relied upon to maintain the technical realm and security management, which included working collaboratively with teams with special responsibilities to initiate and develop vulnerability assessment and carry out penetration testing scenarios for different platform.
- ☑ Identified higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence. Acquired sound understanding of attacks seen over the Internet, root cause analysis and mitigation strategies.
- ☑ **Technical Deliverables:** Conducted network vulnerability assessments to evaluate attack vectors and identified system vulnerabilities.
- ☑ Developed remediation plans and security procedures. Assisted in the rapid execution of information security initiatives by maintaining an appropriate level of prioritization, focus and persistence in an environment of significant change and growth.
- ☑ Assessed the security posture of applications and infrastructure using a variety of assessment tools and methodologies. Tested the ability of network defenders to successfully detect and respond to the attacks. Provided evidence to support increased investments in security personnel and technology.

Security Researcher Trainee ▸ Binary Security Innovative solutions (SecurityTube.net) **Jun 2012 to Aug 2012**

Key Deliverables:

- ☑ **Key Roles & Responsibilities:** Developed attack simulation Proof of Concepts on open-source security tools and frameworks
- ☑ **Achievements:** Gained a proven track record of performing high-quality security research within Information Security

Internship ▸ Kiva Cyber Securities **Feb 2011 to May 2012**

Key Deliverables:

- ☑ **Key Roles & Responsibilities:** Evaluated the security of web applications and internal networks by simulating an attack like an outsider with no authoritative means of accessing the organization's systems and insiders with basic levels of authorized access.
- ☑ Carried out Regular network vulnerability scanning of systems to ensure that configurations are correctly set and that the proper security patches were applied. Identified vulnerabilities or potential threats to each resource. Assisted the management in documenting procedures/standards around Vulnerability Assessment and Application Security testing.

EDUCATION

2012 B.Tech (Computer Science and Engineering), Anurag Engineering College, JNTUH
2008 Intermediate from Board of Intermediate Education, Board of Intermediate Education, Andhra Pradesh, India
2006 Secondary School Education, Kodad Public School, Kodad, Telangana

CERTIFICATIONS

- ☑ Ethical Hacker CEHv 8
- ☑ IBM Certified Deployment Professional - Tivoli Directory Server V6.1
- ☑ QualysGuard Certified Vulnerability Management Specialist
- ☑ Certified EiQ Networks Systems Engineer on SecureVue SIEM

TRAININGS

- ☑ Carbon Black Response Administrator
- ☑ Carbon Black Response Advanced Administrator
- ☑ RedCloak
- ☑ Cylance Optics & Cylance Protect
- ☑ Splunk Fundamentals Training
- ☑ SecureWorks
- ☑ SecureVue

PRESENTATION, TALKS & COURSES

Weaponizing Metasploit Railgun on Windows API

- ☑ Following talk provides quick POC on the usage of Railgun over Windows meterpreter session.
- ☑ Presented this talk in Null Meet held at Tata Consulting Services Hyderabad in Dec 2012.
- ☑ http://www.slideshare.net/chaitanyaanantharapu/metasploit-railguns-presentation-tcs-hyderabad

Penetration Testing with Metasploit (Information Security Course Developed)

- ☑ Created 70 video lecturers on Metasploit usage for beginners in Information Security.
- ☑ The main objective of the video series was to help students become comfortable with extensive usage of Metasploit in their regular assessments within various scenarios.
- ☑ Udemy : https://www.udemy.com/course/penetration-testing-with-metasploit-ethical-hacking-stream/

Enterprise Virtual Lab

- ☑ Developed Virtual testing lab setup which simulates small size enterprise virtual lab running with 45-50 machines with a different set of network configurations and hosted vulnerability. This is purely for learning how different attacks can be conducted in enterprise networks.
- ☑ The main objective of this course is to develop and deploy their own dream lab rather than running 2 or 3 virtual machines simultaneously.

OPEN SOURCE PROJECTS

IOC Scraper

☑ Developed IOC Scraper tool which utilizes IOCPARSER service to fetch IOCs from different vendor Blogs, PDFs, and CSV files. Parsing IOCs is a time-consuming process, using the current script one can automatically extract and aggregate IOCs easily.

Features

- Defanged IOCs: Supports extracting and defanging IOCs.
- Whitelist IOCs: Supports custom whitelisting of IOCs.
- Source Types: Supports a variety of sources such as Blogs, PDFs, CSV, and much more.

Supported IOC Types

- IOC Scraper supports a variety of IOC types.

IOC TYPE	STATUS
ASN	Supported
IPv4, IPv6	Supported
URL, Domain	Supported
Email	Supported
MD5, SHA1, SHA256, File Name	Supported
MAC Address	Supported
MITRE ATT&CK IDs	Supported
YARA Rules	Supported

Source Code: https://github.com/chaitanyakrishna/iocscraper

Subdomain Enum

☑ Developed a simple python script that helps security teams to enumerate subdomains for a targeted domain using SecurityTrails API. Planning to enhance additional futures in an upcoming release.

Source Code: https://github.com/chaitanyakrishna/subdomain-enum

Threat Feed Automator

☑ Threat Feed Automator is developed to crawl IOC's from various sources. The current version of the script can fetch domains and IP Addresses.

Source Code : https://github.com/chaitanyakrishna/ThreatFeedAutomater

Ginger-Chai

☑ Across a range of small-scale assessments, clients request to provide a list of static and dynamic pages within their web application. Ginger-Chai helps these clients in calculating the total number of static and dynamic pages within web applications based on HTTP 200 response code. Results can be exported in .csv format

Source Code: https://github.com/chaitanyakrishna/Ginger-Chai

PERSONAL DETAILS

Date of Birth: 27th August 1991
Languages: English, Telugu, and Hindi
References: Available upon request