Lokesh CK

Principal Cyber Security Consultant

Highly motivated, technologically inquisitive security enthusiast with over **9 years'** experience in technical management of front-line teams such as technical support or incident response, threat intelligence, project implementation, network security, Policy development and implementation and SOAR technology. Proven history of successfully working on solo and group projects.

Employment History

Principal Threat Analyst at Optiv Security
December 2017 — Present

- Responsible for Cybersecurity Incident Discovery and event management, network forensics, IPS/IDS, Firewalls, Content Filtering Technology, DLP, Configuration Management, and Monitoring, End-Point Protection, Database Security and Log Collection and Analysis.
- Working on Python Scapy library for working with network traffic, including network scanning and exploration of an organization network infrastructure using DNS.
- Analyzing and creating threat detection engine rules (snort, yara)
- Provide proactive and accurate data to all stakeholders for internal communication
- Analyzing technical data to extract attacker TTPs, identify unique attributes of malware, map attacker infrastructure, and pivot to related threat data.
- Experience working with analytic visualization tools - Maltego
- Strong understanding of malware families, delivery mechanisms and behaviors.
- Knowledge of operating systems, file systems, and memory on Windows, MacOS, or Linux.
- Extract technical indicators from malware and/or PCAP using technical resources such as VirusTotal, PassiveTotal and DomainTools, as well as internal resources
- An understanding of the MITRE ATT&CK Framework, stages of an attack and sub-techniques. Primarily sub-techniques associated with initial access, network communications, or deployment of malware.
- Support mentoring and technical development of incident response engineers

Contact

Address

Texas, United States

Phone

469 278 8371

E-mail

cklokesh90@gmail.com

Links

LinkedIn

Certifications

- Certified Information Systems Security Professional (CISSP)
- AZ-500
- C | EH
- CrowdStrike Certified Falcon Administrator (CCFA)
- Splunk Enterprise System Admin.

Incident Responder at Pytheus Consulting, India
March 2017 — December 2017

- Providing technical and administration support for Proofpoint Messaging Gateway/Antispam System to secure customer emails infrastructure.
- Was responsible in Integrating Proofpoint TAP alerts into JIRA.
- Providing analysis on various security enforcement technologies including Proofpoint, Sumologic, Cylance, Crowdstrike, Paloalto, and Zscaler.
- Was responsible to analyze, document and report on potential security incidents identified in Client environment.

Security Consultant at Ernst & Young, Bangalore, India
February 2016 — March 2017

- Monitoring incident queues and alerts from various monitoring functions, incidents highlighted via email, phone etc.
- Document and monitoring incidents - Background, progress, next actions.
- Perform remote and onsite live-response activities, document findings, oversee the remediation process to its completion.
- Guide vendors and teams responsible for remediation actions.

Information Security Analyst at Tata Consultancy Services Limited, India
June 2015 — February 2016

- Responsible for identifying frequently occurring security incidents and thereby minimizing the Number and Severity of Security Incidents.
- Responsible for suggesting the teams on what needs to be done on a security incident.
- Analyze and develop new technologies for minimizing security vulnerabilities and risks.
- Provide security consulting services.
- Routinely assess vulnerabilities and coordinating with security specialist and various other stake holders for mitigating the same.

Skills

Python
Very Good

Yara, snort
Very Good

Designing security controls
Very Good

Incident Response
Excellent

SIEM (Splunk, ELK, Qradar)
Excellent

EDR (MDATP, Falcon, SEPM)
Excellent

Open-Source Intelligence (OSINT)
Very Good

SOAR
Excellent

VMS - Nessus and Qualys
Excellent

Cloud Security
Excellent

IT Security Professional at IBM, Bangalore, India
April 2012 — June 2015

- Monitoring of Multiple Security Incidents using SIEM tool (QRadar).
- Analyzing the offenses for Botnet, P2P activity, Virus threat, Trojan, Malwares, Brute force attack, vulnerability, and policy violation activities.
- Technical/Administration support on Symantec messaging gateway for blocking/whitelisting external mail domains, checking/updating spam scores, blocking spam emails and email address, mail encryption, adding domains in TLS, adding users access/block list, managing gateway firewall and creating rules, monitoring quarantine/spam emails, hold emails and released them as per instructions from Client.
- All security events, network transactions and additional contextual information (derived from correlation tests) observed during an attack or violation.

Education

2007-08 - 2011-06

Bachelor of Engineering Technology: Electronics and Communications Engineering

Visvesvaraya Technological University - Bangalore, India