E- 704, Austin County,
Tathawade, Pune – 411033
7999877781
Abhinav.plwl@gmail.com
https://github.com/TheKillChainGuy (Personal)
https://medium.com/@abhinav.plwl (Blog)
https://blog.qualys.com/author/apaliwal (Blog)

ABHINAV PALIWAL

OBJECTIVE

To build a progressive career in the Cybersecurity domain as a Security Leader within a dynamic organization, where I can apply my skills, expertise, and experience to strengthen the organization's security posture and contribute meaningfully to its strategic goals.

QUALIFICATIONS

- Able to identify potential online security risks and its remediation through proper Incident response process.
- Proficient in identifying potential online threats and vulnerabilities, with hands-on experience in driving incident response workflows to contain and remediate cyber risks effectively.
- Experienced across a broad spectrum of cybersecurity domains including Threat Intelligence, Email Security, Endpoint & Network Security, EDR, SIEM, and Vulnerability Management.
- Conduct in-depth Threat Intelligence analysis from OSINT, private sources, and threat feeds, translating them into actionable insights for threat detection, hunting, and executive reporting.
- Lead Threat Hunting activities leveraging the latest threat intelligence and MITRE ATT&CK-aligned TTPs to detect anomalies and adversary behaviors across the environment.
- Skilled in purple teaming methodologies to evaluate detection and response efficacy and identify gaps using tools like Vectr and MITRE Caldera.
- Conduct security product assessments through third-party testing frameworks such as MITRE Evaluations, AV-Test, and AV-Comparatives to measure product performance and coverage.
- Experienced in Security Orchestration, Automation, and Response (SOAR) platforms, designing and implementing playbooks to streamline and automate incident response processes.
- Familiar with malware analysis using both open-source and enterprise tools including REMnux, Cuckoo Sandbox, FireEye ETP, and FireEye NX in sandbox environments.
- Adept at using Python for developing custom scripts and automating repetitive security tasks and processes.
- Knowledgeable in deploying and managing CASB solutions such as Cisco Umbrella to secure cloud access and enforce data policies.
- Comprehensive understanding of defensive security architecture, tools, and technologies

required to protect enterprise infrastructure from evolving cyber threats.

WORK HISTORY

LEAD THREAT RESEARCH ENGINEER AT **QUALYS, PUNE, MAHARASHTRA**

May 2024 to current

SENIOR THREAT RESEARCH ENGINEER AT **VMWARE, PUNE, MAHARASHTRA**

Oct 2021 to May 2024

LEAD SECURITY ANALYST AT **CRANE CO., PUNE, MAHARASHTRA**

March 2018 to Oct 2021

SECURITY ANALYST AT **ATOS GLOBAL IT SOLUTIONS, PUNE, MAHARASHTRA**

August 2015 – March 2018

TECHNICAL SKILLS

INFORMATION SECURITY TOOLS PROFICIENCY

Perimeter/Network Security: Cisco Umbrella, FireEye NX, Cisco FMC IDPS, Websense Proxy

Purple teaming tools: MITRE Caldera and Vectr

Vulnerability Management: Rapid7 InsightVM, Tripwire IP360

Security information and event management (SIEM): Elastic/ELK SIEM

Endpoint Security: McAfee ePO, Symantec Endpoint Protection, VMware Carbon Black EDR, Qualys EDR

Malware Analysis/Protection: Expertise in both manual and automated malware analysis tools

Email Security: Proofpoint Email Gateway, FireEye Email Threat Protection

Scripting: Python

SOAR: Chronicle SOAR

PROFESSIONAL EXPERIENCE

Qualys – Lead Threat Research Engineer (May 2024 to Current)

- Contributed to ISPM product development as the threat-research representative, defining detection logic, correlating risk signals, and shaping attack-path modelling based on real-world threat behaviors.
- Led the Cyber Threat Intelligence (CTI) function, delivering tactical, operational, and strategic intelligence by leveraging OSINT and premium intelligence sources to strengthen the Qualys TruLens platform's detection and analysis capabilities.
- Supported development and enhancement of the Qualys EDR and EPP platforms, contributing threat-informed insights and validation to improve detection logic, response workflows, and product effectiveness.
- Participated in MITRE ATT&CK Evaluation testing, providing threat-scenario design, detection mapping, and validation to ensure clear visibility across adversarial techniques and improve competitive positioning.
- Built automation pipelines for threat-intelligence collection and enrichment, enabling scalable ingestion, correlation, and mapping of TTPs in support of ISPM (Internal

Security Posture Management) product development.

- Integrated CSPM rules into ISPM, expanding visibility into cloud misconfigurations and strengthening unified risk scoring across endpoints, identity, and cloud infrastructure.

VMware – Senior Threat Research Engineer (Oct 2021 to May 2024)

- Working as a part of VMware TAU (Threat Analysis Unit) supported VMware Carbon Black Cloud security platform by deploying new detection and prevention rule within the platform.
- Perform research on latest threat and zero-day exploits to determine if Carbon Black platform have prevention/detection enabled or not.
- Led targeted research efforts with a global team to conduct comprehensive gap analysis via threat emulation and research findings. This leadership resulted in the development and implementation of enhanced rules, detections, and prevention strategies pushed to endpoints.
- Writing research article on Carbon Black community portal for latest threats that demonstrate product capability for that specific threat.
- Improving efficacy of previously built detection/prevention rule by fine tuning for false positives.
- Retiring old non-relevant rules based on current attack surface.
- Performing Adversary Emulation techniques for creating test cases for detection and prevention rules.
- Working on Third-party testing on Carbon Black Cloud security platform that includes MITRE evaluation, AV-Test, AV-Comparatives, etc.
- Involved in performing gap analysis on Carbon Black Cloud security platform to enhance detection and prevention capabilities, using purple teaming methodology.
- Built emulation test cases for MITRE techniques and procedures that include creating scripts and binaries in different programming languages.
- While working on escalation duty investigate and respond to customer escalations regarding the detection and prevention capabilities of the product.

Crane Co. – Lead Security Analyst (March 2018 to October 2021)

- Being part of distributed **Global Information Security** (GIS) team, I am responsible for securing Crane Co. IT infrastructure which include devices from each and every **Business Units** (BU) across the globe using multiple security tools.
- Prioritize, Distribute, Assign alerts to available SOC Analysts. Coordinate with US team and escalate critical/priority Incidents to its remediation.
- Assist in Onboarding of new SOC Analysts and provide insight about GIS team project activities.
- Improving Email security with the help of various tools which includes **Proofpoint Email Gateway**, **Proofpoint Phish Alarm**, and **FireEye ETP**.
- Handing Incidents with proper Incident Response procedure and tools which include **Carbon Black EDR** to analyze the root cause and its remediation.

- Analyzing and remediating security alerts coming from various devices which includes **Wombat Phish Alarm**, **FireEye ETP**, **FireEye NX** and **Carbon Black EDR**.
- Created and improve automated Incident Response playbooks for different use cases in **Chronicle SOAR** platform and use automated playbooks for responding different alerts.
- Performed various activities in **ELK based SIEM** which includes, Creating Correlation rules, responding and investigating alerts, Creating dashboards.
- Created new Incident Response processes and improve old processes which includes creating playbooks, process documentation and presentation to leadership.
- Participated in evaluation, POC & deployment of new security technologies.
- Performed **Threat hunting** activities on Carbon Black EDR and SIEM and create new detections/watchlists/dashboard based on findings.
- Understanding of **CIS Controls** version 7.1 (Centre for Internet Security) to design and deploy security program.
- Working with sandboxing tools for Email Security (**FireEye ETP**) and Network traffic (**FireEye NX**) to ensure Information Security of Crane Co.
- Checking Email Security by creating quarantine rules, Antivirus rules, Blacklisting /Whitelisting Email domains, Spamming rules for junk Emails, monitoring all incoming and outgoing Email traffic, DLP implementation & Encrypted emails with the help of **Proofpoint Email Gateway**.
- Understanding of **Mitre Att&ck** framework and **Cyber Kill chain** and its use cases.
- Ensuring endpoint security with the help of **Bit9** and **Microsoft SCEP** (System Center Endpoint Protection).
- Working with **Cisco umbrella** which is cloud security platform to ensure and adding another layer of security to web traffic to On Premise devices as well as roaming clients.
- Implementing internal Phishing campaign to educate and aware users about latest phishing trends with the help of Wombat **Phish Alarm** tool.

ATOS – Security Analyst (Aug 2015- March 2018)

- Continuously monitored, analyzed and identified security alerts information from all approved security devices, collection techniques and designated system logs.
- Involved in **Cisco Firepower Management Center** IDS/IPS for daily monitoring, analyzing and act on malicious or harmful events.
- Troubleshooting IPS alerts through command line interface
- Rule **suppression**/ dropping traffic, **Blacklisting** IPs through IPDS console.
- Antivirus Management: **McAfee** ePO, **Trend Micro** (Office Scan & Smart Scan) & **Symantec** Endpoint Protection
- Prepared daily weekly and monthly security reports for servers and workstation compliance.
- Checking infection on Servers and workstation and taking remediation actions.
- Working with multiple clients with different geographic locations.
- Knowledge of various ticketing tools including SDM 12.9 (Service Desk Manager),

SDM 12, Service Now and USD (Unicenter Service Desk)

- Monitoring security patch levels of the servers, workstations and network environments, and anti-virus systems.
- Vulnerability Management for vulnerabilities found on Servers and workstations from **Tripwire** scanner.
- Coordination with different teams (Windows/Unix/Web/SAP/Patching /Security)
- Worked in various Linux and Windows environments.
- Performed comprehensive investigations of cyber security breaches.

EDUCATION

PG DIPLOMA DITISS (2015)

PG Diploma from **CDAC ACTS** Pune with specialization in **IT Infrastructure, Systems and Security** with **77**%.

BE INFORMATION TECHNOLOGY (2010-2014)

Bachelor of Engineering from Acropolis Institute of Technology & Research affiliated to RGTU with specialization in Information Technology (Sessional Grade Point Average - 7.10)

SENIOR SECONDARY SCHOOL CERTIFICATE (10+2) (2010)

SSC (10+2) from Priyadarshini School affiliated to Board of Secondary Education Bhopal M.P. with **83.4**%.

HIGH SCHOOL CERTIFICATE (10TH) (2008)

HSC (10th) from Priyadarshini School affiliated to Board of Secondary Education Bhopal M.P. with **85.4**%.

CERTIFICATIONS AND TRAINING

- AZ-500: Microsoft Certified Azure Security Engineer Associate
- EC Council **CTIA** (Certified Threat intelligence Analyst) Professional
- EC Council **CEH** (Certified Ethical Hacker) **V9** Professional
- Certification from Google on “Cyber Intelligence Production”
- Certified in **ITIL®** (Information technology Infrastructure Library) Foundation
- "**Proofpoint Accredited Administrator: Email Protection**" and "**Proofpoint Accredited Administrator: Information Protection**" Certifications.
- Certificate from Carbon Black on successfully completion of "**Carbon Black Protection Administrator Training**"
- Two Certification from Siemplify SOAR on **Siemplify Platform Fundamentals** and **Siemplify Certified SOAR Analyst (SCSA)**
- Fortinet (Network Security Expert) **NSE 1** and **NSE 2** Certified

ACHIEVEMENTS

- Achieved 2nd place in **QIO (Qualys Innovation Odyssey) 2025**, presenting a novel **hybrid attack-path model** demonstrating multi-vector compromise across EDR, Entra ID, and Okta, showcasing cross-domain risk correlation.
- **Certificate of Excellence** award in **Atos** for good initiation for knowledge grasping, proactively involved in process creation, documentation and enabler for smooth knowledge transfer for new joiner.

- Written Appreciation by Crane Co. CIO (Chief Information Officer) for investigating highly escalated email compromise case.

INTERESTS	Reading books, Internet surfing and watching movies.

DECLARATION	I hereby that the above particulars are true to the best of my knowledge & belief.

Place: Pune (Abhinav Paliwal)