ARCHIE CRAWFORD JR

(757) 353-5324 | Archie.Crawford1@gmail.com

A Security Engineer capable of performing real-time log analysis to provide network security for clients and large companies.

Evaluates networks determining the strength of the security environment. Using penetration testing and making use of packet analysis and has in-depth understanding of exploits and vulnerabilities. Analyzes the email environment to determine if it is safe from phishing attacks. Excellent customer service skills and great in a team environment monitoring the health and wellness of network and security devices.

STRENGTHS

- SSO, SAML Integrations (Okta)
- Linux
- Elasticsearch & Splunk
- Vulnerability Management
- Proof Point Email Protection
- MDM, Lookout app
- Palo Alto Firewall, Firemon
- Tenable, Nessus, Qualys, Rapid 7
- Microsoft Azure
- Email Security
- Lookout
- Penetration Testing
- SPF, DMARC, and Dkim
- API Management
- Windows event collection
- AppOmni
- Crowdstrike
- Carbon Black
- LogRhythm SIEM
- SCCM
- RSA Net Witness SIEM
- Jira / Confluence
- Data Loss Prevention (DLP)
- End Point Management

EDUCATION / HONORS & AWARDS

Master of Science, Cyber Security: Liberty University, Lynchburg, VA — Graduated 2017
Bachelor of Arts, Graphic Design: Norfolk State, Norfolk, VA — Graduated 2009
Certifications, Awards & Service: Metro Atlanta ISSA Member, Security +

ACADEMIC EXPERIENCE & ACHIEVEMENTS

MODERNA — ATLANTA, GA (DEC2022 – FEB2024)

SECURITY ENGINEERING

- Create and manage a Windows Event Collector to collect companies Windows logs.
- Create and manage Rsyslog sever to collect logs from Linux servers.
- Integrate Lookout Mobile on Company devices to monitor and manage iPhone.
- Create dashboards within Splunk to view companies SQL logs.
- manage Company USB exception program to allow users to utilize USB devices.
- monitor and manage tenable scans for penetration testing on company websites.
- Work with teams to remove workspace one and integrate Intune.
- Send monthly reports on Metris on mobile statics.

ACE GROUP LLC — ATLANTA, GA (SEPT 2021 –DEC2022)

Security Engineer

- Implement Okta SSO for SAAS Applications
- Installing Windows Event Collector to manage Windows Environment
- Managing Endpoint Inventory, Keeping accountability of active Endpoints
- Building SCCM to Manage Vulnerability Management Program – Via Running PowerShell Scripts
- Manage AppOmni to security cloud applications.
- Used Wireshark to troubleshoot network issues to determine what traffic was following through the network.
- Create and use PowerShell scripts to mitigate issues and vulnerabilities.

COMMUNITY LOANS OF AMERICA — ATLANTA, GA (JAN 2019 – NOV 2021)

Cloud Security Engineer (Full-Time)

- Implemented Nextcloud on remote Centos Servers to create secure document uploads with PII.
- Implemented and monitored Carbon Black, Elasticsearch, and AlienVault.
- Penetration testing on company web applications, with Use of Nessus Vulnerability Scanning

- SSH to configure Cloud Servers and install Apache, MySQL, and PHP

Unisys — Augusta GA, (NOV 2018 – JAN 2019)

Cyber Security Analyst (Contract)

- Analyzed events generated through LogRhythm SIEM to determine if network traffic is malicious.
- Applying knowledge of a client's security policies and procedures to detect, analyses and prevent both internal and external security breaches using SIEM and other security event monitoring tools
- Manage Firewall rules through Fortinet Firewall software

AMERICAN EXPRESS — REMOTE (OCT 2016 – OCT 2018)

Inter Internet Security Specialist (Email Security Team) (Contract)

- Primary duties are to work on infrastructure security projects focusing on email security
- Work within Proofpoint to manage email routing for security purposes
- Manage SPF Records and Defense of Domains within the company.

DATA PATH — DULUTH, GA (OCT 2016 – NOV 2017)

Cyber Security Operations Center Specialist (Full Time)

- Analyzed PCAPs to determine network intrusions through Alien Vault SIEM.
- Perform accurate and precise real-time analysis and correlation of logs/alerts from a multitude of client devices with a focus on the determination of whether events constitute security incidents.

DELL SECURE WORKS — Atlanta, GA (Aug 2015- April 2016)

Security Operations Center Ops Sr Analyst Inter Internet Security Specialist (Full Time)

- Monitored and responded to security incidents from network IDS/IPS devices and worked directly with vendors to troubleshoot network security intrusions.
- Interact proprietary and commercial consoles, both local and remote with over 1,000 different clients.
- Provided Log analysis to clients to determine whether it was true positive or false positive.

AT&T — Atlanta, GA (Jan 2015 -Aug 2015)

Customer Advocacy Manager (Internship)

- Analyze trouble tickets and push tickets through completion, implementing fixes along the way.
- Managed a team of techs and audited tickets to ensure quality analysis.
- Provide customer support and troubleshooting assistance for business customers with faulty voice and internet related services.

UNITED STATES ARMY — Virginia, VA (Jul 2007-May 2014)

Company Commander / Project Manager (Full-time)

- Information security officer with-in a company of 120 employees Briefing security techniques and teaching information security classes to employees while keeping all employees up to date on training.
- Managed physical security program and maintained a first time go on company audits.