Antonio Hicks

205 Farm Manor CT.

Lawrenceville, GA. 30045

419.787.9526

[tonyhicks3240@gmail.com](mailto:tonyhicks3240@gmail.com)

**DOB: 03/13**

**SSN#:3240**

**Grad Date: 2010**

**LinkedIn:** [**https://www.linkedin.com/in/antonio-hicks-88a46130/**](https://www.linkedin.com/in/antonio-hicks-88a46130/)

**US Citizen**

**SUMMARY OF QUALIFICATIONS:**

* Personal attributes: dedication, integrity, and strong work ethic. A fast learner that adapts well to new challenges and job requirements. Able to approach extreme challenges with composure and clarity.
* Well organized, detail oriented and efficient. Able to plan, prioritize and complete multiple tasks in a thorough, efficient & accurate manner.
* Extremely service oriented and self-starting individual with a strong track record of success in problem solving skills.
* Confident, articulate and persuasive team-builder able to motivate and communicate effectively to maintain integrity of mission and vision while achieving exceptional business performance.

**EDUCATION/TRAINING:**

**Westwood College** *Information Systems Security* ***Bachelor of Science***

**CERTIFICATIONS:**

CEH (Certified Ethical Hacker); Security+CE; ITILv3; Qualys Guard Certified Specialist; Cyberark PAS certified Level2: Defender

**RELEVANT EXPERIENCE:**

09/2022-Present **Cyberark EPM Engineer**, Collabera, *Lawrenceville, GA*

* Assist in operationalizing CyberArk EPM deployment including - agent deployment, policy creation, management and tuning, troubleshooting and documentation
* Locate and evaluate software in various repositories for packaging, centralization or deletion
* Bulk create elevation policies with CyberArk EPM, using a best practice approach
* Work with application owners and IT admins to test and sign off on their applications
* Provide regular updates on project progression and blockers
* Integrate CyberArk solutions with other security tooling including IAM, endpoint management, logging and monitoring

01/2022-08/2022 **CyberArk - Technical Business Analyst**, 3 Dots (Metlife), *Lawrenceville, GA*

* Clean-up of Safe Structure
* Naming changes and corrections to team safes, application Safes and accounts
* Name conventions to match Cherwell system – source of truth
* Documentation processes
* Minor version upgrades
* Create custom connectors
* Patching component servers
* Create accounts and safes adding users
* Set up platforms for accounts and rule for password length and duration
* Compliance for SOCS and PCI – troubleshooting failed accounts.
* Day to Day operational functions

08/2021-01/2022 **IAM CyberArk Security Engineer,** Talentburst(Synopsys)*, Lawrenceville, GA*

* Assist in the operationalization of CyberArk EPM deployment including: agent deployment, policy management and tuning, troubleshooting and documentation.
* Locate and evaluate software in various repositories for packaging, centralization, or deletion.
* Create elevation policies with CyberArk EPM, using a best practice approach.
* Work with application owners and IT admins to test and sign-off on their applications.
* Provide regular updates to management on project progression, milestones and blockers
* Help execute operational tasks to support overall IAM program

02/2020-09/21 **Sr. Security Analyst,** *Primerica, Duluth, GA.*

* Receiving alerts from IPS (FireEye), DLP (Symantec), EDR (Carbon Black), TAP Alerts (ProofPoint) I conduct investigations to determine if there is anything suspicious or malicious from the notifications coming from the list of security tools, so that they can be remediated or flagged as false positives.
* Correlate events and gathering more information to make determinations in SIEM (QRadar)

**IAM CyberArk Admin:**

* Perform the day-day activities related to CyberArk including the development, testing and roll-out phase activities of the implementation and support.
* Implementing and supporting Application Identity Management (AIM/AAM) installing and implementing the CyberArk AIM module, specifically installing Credential Providers on servers.
* Vaulting AWS, service and application accounts
* Perform component installation (CPM, PSM and PVWA).
* Configure Load Balanced setup for PSM and PVWA.
* Perform DNA Scan, as per client requirements to get an idea of Privileged accounts present in environment.
* Create Safe Design and Dual Control procedures.
* Configuring Master Policy.
* Integrate ID’s across various OS platforms into Cyber Ark.
* Manage operations of CyberArk components and perform maintenance of the same.
* Fine tuning existing CPM and PVWA policies depending on changing environment.
* Provide L3 support during severity issues.
* Version Upgrade
* Managing DR Site

04/2019-02/2020 **Security Operations Center Tier 2 Analyst**, *Pinnacle Staffing (Remote Contract)*

* Assist analyst investigation and ticket creation efforts. Provide daily monitoring and alerting of events that occur within the near real time environment
* Manage the SOC mailbox, and monitor and analyze the emails for threats including phishing and malware, and escalates per procedure
* Monitor, evaluate, and assist with the maintenance of assigned security systems in accordance with industry best practices to safeguard internal information systems and databases
* Stay informed of current events in the security industry including the latest exploits and threats as well as preventative measures, remediation, and restoration techniques
* Oversee and ensure P1 and P2 incidents are handled according to operational procedures. Document areas of improvement through after-action reports and work with necessary parties to resolve any findings
* Identify improvements within processes, procedures, policies, staffing, training, and tools to improve efforts and daily operations
* Assist in developing and maturing the future services and capabilities of the SOC, using Qradar SIEM
* , Carbon black EDR, ProofPoint Email gateway, Checkpoint Firewalls and other security tools.

07/2015-02/19 **Cyber Security Analyst**, *Country Financial, Alpharetta, Georgia*

* Respond to CSIRT mailbox, escalating and remediating incidents
* Create objects and rules from request for Checkpoint Firewalls; placing SAM blocks on IPs that are scanning the network
* Using Bluecoat Reporter, scheduled reports malicious botnets, application downloads and potential infections.
* Monitor and investigate TAP alerts from Proofpoint. Remediating malware infections through virus scans using McAfee Anti-virus and tools such as Virustotal, Malwr and others to investigate malware alerts. Respond to phishing alerts.
* Use ProofPoint to blacklist email addresses block senders and IP addresses associated with SPAM. Monitor spoofing and geo-location folders for suspicious email.
* Checking shared drives for PII and escalate for quarantine or mark as false positive with McAfee DLP. Now using Symantec DLP.
* Monitor security events and logs from a variety of sources including firewalls, network and data at rest DLP, IDS/IPS, network devices, system logs, and other data feeds in order to detect security anomalies, provide analysis and respond with appropriate mitigation to prevent a security incident.
* Interface with Security Risk Management and provide detailed analysis and information on applicable weaknesses and vulnerabilities.
* Using Qualys we are scanning and reporting to different teams the vulnerabilities thy may have. Checking to see if there are any compensating controls in place and to make sure patching stays on schedule.
* Remediate and respond to Carbon Black alerts to files that are blocked, creating and tuning policy.
* Investigate and remediate escalations from MSSP, Secureworks.
* SIEM: Tibco Loglogic / QRadar

**IAM CyberArk Admin:**

* Perform the day-day activities related to CyberArk including the development, testing and roll-out phase activities of the implementation and support.
* Implementing and supporting Application Identity Management (AIM/AAM).installing and implementing the CyberArk AIM module, specifically installing Credential Providers on servers.
* Vaulting AWS, service and application accounts
* Perform component installation (CPM, PSM and PVWA).
* Configure Load Balanced setup for PSM and PVWA.
* Perform DNA Scan, as per client requirements to get an idea of Privileged accounts present in environment.
* Create Safe Design and Dual Control procedures.
* Configuring Master Policy.
* Integrate ID’s across various OS platforms into Cyber Ark.
* Manage operations of CyberArk components and perform maintenance of the same.
* Fine tuning existing CPM and PVWA policies depending on changing environment.
* Provide L3 support during severity issues.
* Version Upgrade
* Managing DR Site

04/2014-07/2015 **SOC Analyst,** *Fiserv, Atlanta, Georgia*

* Perform analysis of log files. Includes analysis of system resource access using Arcsight and Checkpoint Smartview Tracker also firewall health checks.

 Monitor network security events received from alerts in Sourcefire IDS/IPS and Alertlogic, and then take appropriate action based on security policy. Also monitoring the network for any anomalies and malicious/suspicious activity.

* Perform vulnerability scans of devices sitting on the network using Qualys, gather reports and determine security levels from QID’s
* Blocking/blacklisting URL’s on the Bluecoat proxy, check proxy health and traffic
* Strong analytical and problem solving skills
* Incident response using Remedy ticketing system and Alarmpoint notifications to join bridges to remediate incidents.
* Investigate and remediate SOC tickets from Dell Secureworks.

07/2013-04/2014 **Security Analyst,** *Fiserv, Atlanta, Georgia*

* Maintain certificate management operational guidelines and processes to directly support Fiserv’s security architecture and design to protect web sites, applications and the integrity of financial transactions.
* Support existing SSL certificate management security solutions and partner with the security engineering team for the implementation and integration of any new enhancements made to Certificate Management security solutions in support of improving overall enterprise security.
* Ensure certificate management security tools and solutions hardware/software/devices are operating effectively and updated in a timely manner.
* Develop and maintain certificate management operating guidelines and procedures in support of Fiserv’s policies, standards and guidelines.
* Determine appropriate levels of certificate management security configuration, controls and monitoring.
* Use appropriate and effective measures to respond to certificate management network alerts and incidents.
* Support the maintenance and deployment of new certificates, renewals and revocations in multiple ETG data centers.
* Understand the latest key and certificate management threat techniques and support appropriate countermeasures, configurations and awareness.
* Support X.509 certificate management technologies on multiple platforms for internal/external clients.
* Overall central management of certificate management solutions.
* Work with members of all BU and ETG staff to support the enterprise approach to key management and certificates.
* Ensure the confidentiality, integrity and availability of the data residing on or transmitted to/from/through enterprise networks.
* Perform certificate management ticket queue monitoring, resolution and prioritization, maintain diagrams and documentation as appropriate and support data reviews, auditing and maintenance activities
* SSL Certificate experience (root, intermediate, CSAPI, PKCS, certification stores, chains.)
* Foundational network knowledge including load balancers, bindings and system configuration
* PKI and SSL exposure and experience, including a strong preference for industry tools used for Certificate Lifecycle Management (Venafi, Trustwave.).

12/2012-06/2013 **Security Analyst,** *Park n’ Fly, Atlanta, Georgia (Contract)*

* Monitor IPS for security related events and implemented blocks based on analysis of traffic patterns using Sourcefire.
* Assist in developing, defining, and directing the information security awareness program. Definition and implementation of technology and policy architecture.
* Coordination of Patch Management and vulnerability testing. Proactive determination of trends related to predictive pathways, threat agents and attack vectors.
* Monitor and manage Symantec Endpoint anti-virus software on all endpoints using central management console
* Provide Information Security training to new employees and administer semi-annual Security Policy awareness training.
* Use of ticketing system to efficiently meet the clients’ needs.
* Installed mobile device encryption technologies to employee company mobile devices.
* Acceptable use/ Security policy creation and revision
* Physical security administration, configuration and installation of Genetec and Axis camera and NVR systems.
* Document issues and their resolution in the incident management system

.

5/2012-12/2012 **Security Administrator***, Home Depot, Atlanta, Georgia* *(Contract)*

* Monitor and audited Symantec Endpoint anti-virus software on all remote computers using central management console.
* Utilize SIEM Log Rhythm to troubleshoot and identify issues
* Monitor IDS and IPS for security related events and implemented blocks based on analysis of traffic patterns
* Document issues and their resolution in the incident management system
* Utilize remote tools to troubleshoot and identify issues
* Use of ticketing system to efficiently meet the clients’ needs
* Eyes on glass monitoring of different security technologies.

6/2011-4/2012 **Jr. Security Analyst,** *Staley Technologies, Norcross, Georgia*

* Creating playbooks and procedures, documenting the process.
  + - Monitor IPS for security related events and implemented blocks based on analysis of traffic patterns
* Remove virus from workstation while protecting data integrity
* Document issues and their resolution in the Incident Response program.
* Handled abuse email through Abusix security tool