# Jacob B. Henson

Email: jacob@henson.me
Mobile: (256) 361-9211
Clearance: Top Secret

With over 20 years of extensive experience in Cybersecurity and IT, adept at leading teams and overseeing projects. Recognized for possessing a focused, calm, and level-headed approach to challenges. Demonstrated track record of successful project-oriented development, governance, and risk management, all tailored to the evolving needs of a growing business. Equipped with in-depth expertise in adhering to various compliance standards, including NIST SP 800-53, NIST SP 800-171, ISO 20,000, CSC Top 20, and NIST Cybersecurity Framework. Proficient in conducting IT due diligence and effectively integrating mergers and acquisitions. My ultimate passion lies in problem-solving and optimizing processes to drive efficiency and innovation.

## Experience

**Cybersecurity Engineer, ECS Federal; Huntsville, AL July 2022 – Present**

- As a lead SIEM engineer, I take charge of overseeing professional service engagements and managing service provider (MSP) customers, working collaboratively with a team of engineers.
- Implementing configuration management using Ansible to streamline and automate processes.
- Set up and maintain Elasticsearch clusters as well as Swimlane clusters for seamless operations.
- Configuring Fleet and Elastic agent policies with both standard and custom integrations to optimize operations.
- Deploy machine learning jobs with the objective of detecting anomalies.
- Ensuring compliance and security standards by applying STIGS to Swimlane and Elasticsearch platforms.
- Evaluating and enhancing the performance and security of customers' Elasticsearch environments by providing expert guidance.
- Employing Docker for containerization and establishing immutable pipelines for enhanced efficiency.
- Configure PagerDuty for multiple teams and workflows to ensure smooth incident management.
- Develop custom solutions using AWS SNS, SQS, and Lambda functions to address specific requirements.
- Create and maintain comprehensive documentation of security configurations, procedures, and incidents.
- Facilitate and lead Scrum meetings for the SIEM team while collaborating closely with project managers to prioritize and incorporate tasks into the backlog.

**INFOSEC Solutions Provider, VIKTech; Huntsville, AL April 2019 – June 2022**

- Serve as CND Contractor Lead for a Missile Defense Agency (MDA) Directorate.
- Work with multiple teams to report and address compliance and information assurance vulnerability management (IAVM) findings.
- Validate vulnerability assessments, and artifacts in eMASS, ePO, and ACAS and make a recommendation to address findings.
- Coordinate with multiple teams to track, document, and respond to incidents.
- Develop and Maintain CND Strategic Plans, Policies, and Procedures.
- Support Risk Management Framework (RMF) Assessment and Authorization (A&A) processes in our team.

Email: jacob@henson.me
Mobile: (256) 361-9211
Clearance: Top Secret

- Develop and deliver briefings to Directorate leadership.
- Aggregate data from multiple data sources using PowerBI, Excel, Power Query, and PowerShell.

**Chief Information Security Officer (CISO), HII Technical Solutions; Huntsville, AL Feb 2016 – Apr 2019**

- Directed the Cybersecurity Program and Risk Management that includes the Risk Management Framework (RFM) supporting multiple entities in a global division.
- Team Lead for the division's Incident Response Team. As the lead, I am responsible for coordinating with multiple departments to bring an incident to closure. Provide written and verbal briefings and presentations to business leaders about incidents.
- Directed IT governance for the division that aligns with HII, compliance frameworks (e.g., ISO 9001, ISO 20000, and NIST SP 800-171), and contractual requirements (e.g., DFARS 252.204-7012) to align with business objectives. Advise senior leadership on governance, risk management, and regulatory compliance requirements.
- Develop a division-wide Vulnerability Management Program. My team developed governance and processes to reduce the number of vulnerabilities across the division. The program requires interfacing with multiple business units, application owners, and stakeholders to remediate vulnerabilities.
- Led the implementation of Multi-Factor Authentication across the various organization in the division. Managed the initial distribution and developed procedures for continued distribution for future users. My team distributed to CONUS and OCONUS users in than more 70 locations.

**Information Assurances and Cybersecurity and ISSM, Camber; Huntsville, AL 2014 Feb – 2016 Feb**

- Developed, implemented, and maintained Business Continuity and Disaster Recovery Policies and Procedures.
- Managed process and acted in the lead role for Computer Incident Response Team (CIRT). Perform forensics on compromised machines and networks, malware analysis, and reporting relating to security incidents.
- Install, maintain, and manage security technologies including FireEye NX, Carbon Black Enterprise Response, Carbon Black Enterprise Protection (Bit9), Splunk, Elastic, Logstash, Kabana, Encase, Nessus, and Suricata.
- Recommended preventive, mitigating, and compensating controls to ensure the appropriate level of protection and adherence to the goals of the overall information security strategy.
- Configure and Administer BMC Footprints to support our ISO 20000 requirements.
- Developed and maintain corporate information security and privacy policies.
- Prepare Information System Security Plans, Protection Profiles (SSPs and MSSPs). Interface with the Defense Security Service (DSS) concerning Security Plan approvals for handling, safeguarding, transmitting, receiving, and generating classified information.
- Manage COMSEC material and accounts.

**Manager of Business Systems and ISSO, Camber; Huntsville, AL May 2006 – Feb 2014**

Email: jacob@henson.me
Mobile: (256) 361-9211
Clearance: Top Secret

- Prepare Information System Security Plans, Protection Profiles (SSPs and MSSPs). Interface with the Defense Security Service (DSS) concerning Security Plan approvals for handling, safeguarding, transmitting, receiving, and generating classified information.
- Manage COMSEC material and accounts.
- Designed, develop requirements, software development, debug many internal systems to integrate different business systems. (Websites, Restful APIs, and Services)
- Install, support, and operate many business systems including Microsoft SharePoint, Microsoft SQL, Deltek (Costpoint, Budget, and Planning, Govwin, Time and Expense), Privia, Team Foundation Server, and GitHub Enterprise.
- Install, support, and operate cybersecurity technologies including FireEye NX, Carbon Black Enterprise Response, Carbon Black Enterprise Protection (Bit9), Snort, Cuckoo Sandbox, and Splunk (dashboards, reports, custom search commands).
- Provide support and recommendations to HIPAA security assessment and audit. Draft documentation support to ISO 9000, and ISO 20000.

**Developer, College of Business at Auburn University; Auburn, AL Jan 2004 – May 2006**

- Web Developer and Database Administrator
- Responsible for maintaining the College of Business IT infrastructure, and the design of new web-based applications to aid the College of Business in everyday tasks, including the web-based scholarship application process and an online software request form.
- Provided various IT services to the College of Business staff including web surveys, database support, and personal site maintenance.
- Provided custom IT support as needed to assist the College of Business staff.

**Developer, Commerce Networks | Auburn, AL | Aug 2001 – Jan 2004**

- Web Developer
- Developed custom dynamic web applications to meet customers' requirements.

**Technician, Byte-Me Computers; Guntersville, AL | Jan 1995 - Aug 1999 (20 Hours Weekly)**

- Provided custom IT and computer resource design, development, testing, and integration.
- IT Help Desk Support and real-time troubleshooting of IT architectures.
- Operation System and Software maintenance, upgrades, custom configuration setups, and cybersecurity software for penetration and snooping prevention.

## Education

- Auburn University - Bachelor of Computer Science 2005
- ISC2 - CISSP (573982)
- CompTIA - CySA+ (6F817M8GSCF4QBGJ)
- Virtual Hacking Lab - Penetration Testing Course (1998569597)
- Virtual Hacking Lab - Penetration Testing Course Advanced+ (1981030295)
- Offense Security Certified Professional (OSCP) (OS-101-49877)

# Jacob B. Henson

Email: jacob@henson.me
Mobile: (256) 361-9211
Clearance: Top Secret


- AWS Certified Cloud Practitioner (QGJ136JKPB44QK3V)
- Elastic Certified Engineer (55067194)
- Elastic Certified Observability Engineer (69868860)
- Elastic Certified Analyst (61828098)

## Skills

Baselining, Change Control, Cybersecurity Operations, Data Aggregation, Endpoint Detection & Response, Incident Response, Information Assurance, Log Management, Mentor, Policy Development, Project Management, Risk Management, Software Development, Standards and Frameworks, Team Leader, Vulnerability Management

## Expertise

ACAS, Active Directory, ASP.NET, Bash, Bit9, BMC FootPrints, C#, Carbonblack Protection, Carbonblack Response, Costpoint, Cyphort, Dell Kace, Deltek Time and Expense, Digital Certificates, Elasticsearch, Kibana, Filebeat, Logstash, Metric Beat, eMASS, ePO, FireEye HX, FireEye NX, Git, HBSS, PowerShell, Project, Python, Security Onion, SharePoint, Snort, Splunk, SQL Server, SQL, SSH, SSL, Suricata, Tenable Security Center, Visual Studios, Power Query, PowerBI, Swimlane, Docker, Ansible