James Benitez

Cyber Security Engineer, VP

(704) 555-0186 james.benitez@email.com
linkedin.com/example/jamesbenitez Charlotte, North Carolina 28202

STRENGTHS

Telemetry Quality
Built source-readiness checks for timestamps, schemas, completeness, and retention; analysts gained dependable evidence during onboarding reviews.

Cross-Team Delivery
Brought application, cloud, infrastructure, security, and vendor peers together; shared ownership cleared stubborn field-mapping gaps.

Data Troubleshooting
Used Kusto queries, regular expressions, and sample events to restore malformed records; engineers sought help on difficult parsing defects.

Operational Documentation
Created runbooks, mappings, checklists, and source templates; partners had a practical reference for repeatable onboarding work.

Security Visibility
Connected identity, endpoint, network, application, and cloud telemetry; detection teams gained stronger coverage for investigations and risk reporting.

SKILLS

SIEM Onboarding
Azure Data Explorer | Log Analytics
Kusto Query Language | Python
PowerShell | JSON | XML | CSV
Regular Expressions
Schema Mapping
Data Normalization
Data Validation

SUMMARY

Cyber security data engineering leader with more than seven years building reliable telemetry pipelines across cloud and on-premises financial services environments. Leads SIEM onboarding, **Azure Data Explorer** and Log Analytics delivery, data validation, parsing, normalization, enrichment, and schema mapping for network, endpoint, identity, application, cloud, and infrastructure sources. Partners with application, infrastructure, cloud, security, vendor, and business teams to resolve data quality issues and improve monitoring coverage. Hands-on work includes Python, PowerShell, Kusto Query Language, JSON, XML, CSV, regular expressions, **infrastructure-as-code**, automated deployment, threat detection, **incident response**, vulnerability management, retention, auditability, and data integrity. Ready to help a regulated financial services team build dependable security data foundations, strengthen **cyber risk visibility**, and support confident operational decisions.

EXPERIENCE

Cyber Security Data Engineering Lead

HarborPoint Capital Services January 2024 - Present Charlotte, North Carolina

Leads security telemetry engineering across cloud and **on-premises** environments, supporting SIEM monitoring, **threat detection**, incident response, compliance reporting, and cyber risk visibility for 18 business applications.

- Built Python and PowerShell validators for JSON, XML, CSV, and log telemetry before Azure routing.
- Established source checks for completeness, timestamps, schemas, **timeliness**, and retention during onboarding and audits.
- Coordinated application, infrastructure, **cloud**, security, and vendor teams across identity, endpoint, network, and cloud sources.
- Used Kusto Query Language and **regular expressions** to isolate parsing defects and restore delayed security events.
- Embedded pipeline configurations and deployment checks in **infrastructure-as-code** workflows for repeatable source releases.
- Documented data mappings and onboarding procedures, giving partners a shared reference for ownership and field gaps.

Senior Security Data Engineer

BlueRidge Payment Network August 2021 - December 2023 Raleigh, North Carolina

Managed **security log onboarding** for payment, authentication, network, and cloud platforms while balancing incident response needs with planned engineering delivery and regulated data controls.

- Designed **Azure Data Explorer** ingestion patterns with **normalization**, enrichment, duplicate detection, and field validation.
- Performed **telemetry gap assessments** with detection and vulnerability teams, recommending sources for privileged access visibility.
- Diagnosed schema drift and delayed events through Kusto queries, Python diagnostics, and source reviews.
- Created runbooks, source templates, operational checklists, and data dictionaries for consistent engineering handoffs.
- Traced event lineage from collection through analytics, documenting **integrity** and **retention** considerations for payment investigations.
- Connected external providers with internal engineers, turning unresolved onboarding issues into clear ownership and action plans.

Security Operations Engineer

Crescent Harbor Bank June 2019 - July 2021 Richmond, Virginia

Telemetry Gap Analysis

Threat Detection

LANGUAGES

English — Native

Spanish — Intermediate

MY CAREER

- Cyber Security Data Engineering Lead at HarborPoint Capital Services (2.7 Years)
- Senior Security Data Engineer at BlueRidge Payment Network (2.3 Years)
- Security Operations Engineer at Crescent Harbor Bank (2.1 Years)
- Cybersecurity Data Analyst at Piedmont Financial Technology Group (11 Months)

Supported **security operations** across endpoint, identity, firewall, proxy, server, and cloud logs feeding enterprise SIEM and **security analytics** workflows.

- Wrote PowerShell and Python tests for source connectivity, expected fields, and incomplete telemetry.
- Investigated ingestion failures with Kusto Query Language, **regular expressions**, and sample-event analysis.
- Partnered with infrastructure and application owners on source requirements, collection **validation**, and controlled releases.
- Connected authentication, endpoint, network, and application events during **incident response** and vulnerability investigations.
- Maintained evidence for logging, retention, auditability, and **data integrity** controls during financial examinations.
- Shared clear technical findings with engineering partners, helping restore analyst access to actionable security records.

Cybersecurity Data Analyst

Piedmont Financial Technology Group June 2018 - May 2019 Greensboro, North Carolina

Analyzed security event feeds and supported controlled telemetry changes through schema validation, event testing, documentation, and data quality reporting for security operations.

- Analyzed identity, network, endpoint, and infrastructure feeds for missing fields and timestamp issues.
- Built **CSV** validation reports and Python parsers comparing source schemas with **SIEM** mappings.
- Documented event formats, normalization rules, retention expectations, and escalation paths for technical stakeholders.
- Used Kusto Query Language and **regular expressions** to test events after mapping updates.
- Prepared test cases and recorded validation outcomes for controlled telemetry changes and release reviews.
- Presented recurring **data quality** trends, helping prioritize automation, source maintenance, and **monitoring** coverage.

PROJECTS

Enterprise Telemetry Reliability Program 2025

Partnered with security, cloud, and application peers to standardize source readiness across 18 applications. Built shared validation evidence for completeness, integrity, timeliness, schema consistency, and retention, giving analysts and audit partners a dependable view of telemetry health.

Payment Security Data Modernization 2023

Worked with detection engineers and external providers on a shared onboarding backlog. Improved Azure Data Explorer ingestion through normalization, enrichment, duplicate detection, and lineage checks supporting threat investigations and regulated payment operations.

LEADERSHIP & AWARDS

- Security Engineering Excellence Award, HarborPoint Capital Services, 2025
- Operational Reliability Recognition, BlueRidge Payment Network, 2023
- Crescent Harbor Bank Risk and Controls Achievement Award, 2020

EDUCATION

Bachelor's Degree in Information Technology

Appalachian State University GPA: 3.5 2018 Boone, North Carolina

Coursework: *Cybersecurity, Database Management, Network Administration, Systems Analysis*

CERTIFICATIONS

- Microsoft Certified: Azure Security Engineer Associate 2024

- Microsoft Certified: Azure Data Engineer Associate 2023
- GIAC Security Essentials (GSEC) 2022
- Microsoft Certified: Azure Fundamentals 2020

TECHNICAL SKILLS

- **SIEM and Analytics:** SIEM onboarding, security analytics, Log Analytics
- **Azure Data Services:** Azure Data Explorer, Azure Monitor, Azure cloud
- **Programming and Scripting:** Python, PowerShell, regular expressions
- **Data Formats:** JSON, XML, CSV
- **Data Engineering:** Data ingestion, normalization, transformation
- **Data Quality:** Data validation, schema mapping, integrity checks
- **Query Languages:** Kusto Query Language, security queries, analytical queries
- **Security Telemetry:** Network logs, endpoint logs, identity logs
- **Cloud and Infrastructure:** Cloud logging, on-premises systems, infrastructure-as-code
- **Security Operations:** Threat detection, incident response, vulnerability management
- **Governance and Controls:** Logging, retention, auditability
- **Deployment and Documentation:** Automated deployment, pipeline configuration, technical documentation

PROFESSIONAL AFFILIATIONS

- Mentor, Charlotte Cybersecurity Professionals Network, 2024 - Present; connects practitioners with practical security data guidance.
- Technical Reviewer, Piedmont Financial Technology Group Security Automation Forum, 2020 - 2021; strengthened peer review of automation work.
- Volunteer Instructor, Appalachian State University Cybersecurity Career Panel, 2019 - Present; shares career lessons with emerging professionals.

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST