ERIC THOMPSON, CISSP

Professional Summary

Senior Cybersecurity Engineer | Data Protection & Classification | CISSP

Enterprise cybersecurity professional with 20+ years of experience supporting large financial institutions and regulated environments. Deep expertise in data protection controls, vulnerability management, platform onboarding, access governance, and security tooling implementation. Proven ability to design, deploy, and operationalize enterprise security technologies, support data classification and scanning controls, and lead complex security initiatives aligned with NIST, FDIC, and banking regulatory standards. Recent work includes leading a government account through a SOC 2 audit and performing a HIPAA compliance review.

Data Protection & Security Operations

- Data Scanning & Classification Controls (Structured & Unstructured Data)
- Data Risk Taxonomy Alignment (Banking / Regulatory Environments)
- Platform Onboarding & Server-Based Application Deployment
- Security Tool Configuration & Operationalization
- Role-Based Access Control (RBAC) & Identity Integration
- Control Execution, Evidence Collection & Ratings Support
- Change Management & Operational Handoffs

Core Competencies

- Security Governance • Risk Management • Regulatory Compliance • Vulnerability & Patch Management• Configuration Management • Identity & Access Management • Data Protection • NIST & ISO Frameworks • Incident Response • Cybersecurity Strategy

Professional Experience

Cybersecurity Consultant

Kyndryl – New York, NY | March 2020 – Present

- Supported enterprise data protection initiatives by implementing and operationalizing security controls that protect sensitive data across applications, servers, and user environments.
- Assisted with onboarding new security platforms, including role group configuration, server-based installations, access alignment, and operational readiness.
- Executed ongoing security scanning, classification, and control validation activities to maintain compliance with internal risk ratings and regulatory requirements.
- Partnered with application teams and infrastructure owners to align security tooling with business workflows and data usage patterns.
- Contributed to planning, testing, and implementation phases of cybersecurity technology projects, ensuring smooth transition to steady-state operations.
- Provided technical guidance and documentation to support audits, attestations, and control evidence requirements.
- Led a government account through a SOC 2 audit in 2025, coordinating readiness across control owners, mapping controls to Trust Services Criteria, gathering evidence, and working directly with the auditors to bring the engagement to a successful completion.
- Performed a HIPAA compliance review for a government account, assessing administrative, physical, and technical safeguards against the Security and Privacy Rules and documenting gaps and remediation recommendations for the account team.

ERIC THOMPSON, CISSP

Systems Engineer – Patch Governance & Security Operations

Truist Bank | July 2010 – March 2020

- Led enterprise security operations supporting over **50,000 endpoints**, ensuring continuous protection of systems handling sensitive and regulated data.
- Deployed, configured, and managed security tooling used to scan, assess, and enforce compliance across Windows, Linux, and AIX platforms.
- Supported access governance and role-based authentication models across mixed authentication environments (Local, LDAP).
- Partnered with cybersecurity, server, and application teams to remediate vulnerabilities and support enterprise security initiatives, including zero-day response efforts.
- Supported control execution, reporting, and evidence generation aligned with internal risk governance and regulatory expectations.
- Implemented privileged access controls (CyberArk) to protect sensitive system and data access in line with least-privilege principles.

Senior Information Security Analyst

Federal Reserve Bank | Feb 2002 – March 2010

- Conducted enterprise vulnerability assessments and penetration testing across ~30,000 endpoints in a highly regulated financial environment.
- Supported incident response investigations involving data exposure risks, forensic analysis, and executive-level reporting.
- Assisted in the design and rollout of privileged access management and multi-factor authentication solutions.
- Contributed to threat modeling discussions and security control design for applications and infrastructure platforms.
- Led the transition of legacy security policies to a NIST-aligned framework supporting standardized control execution and governance.

Other Roles at Federal Reserve Bank

Atlanta, GA | 1993 – 2002

- Payor Bank Services Supervisor
- PC Support Specialist

Military Experience

United States Air Force | Jan 1990 – Aug 1993
Communication / Navigations / Avionics Engineer

ERIC THOMPSON, CISSP

Education & Certifications

- CISSP
- A+ Certification
- ITIL
- Computer Forensic Training
- Communication & Navigations Systems – Keesler AFB Avionics Technical School

Technical Skills

Operating Systems: Windows, Linux, AIX, zOS
Applications: Tenable, NESSUS, SCCM, ServiceNow, PowerShell, Qualys, CyberArk
Methodologies: ITIL, Agile
LLMS: Cluade, ChatGPT, Grok, CoPilot,
Standards: HIPAA, SOC 2, NIST, ISO/IEC 27001, PCI DSS, GDPR, IRS Publication 1075