

## Lead of Cybersecurity Data Protection & Analytics

*Various Locations - U.S.*

### **Summary**

The Lead of Cybersecurity Data Protection & Analytics will operate as a member of the [The Edge] technology Cybersecurity leadership team reporting to the Chief Information Security Officer (CISO). This role contributes [The Edge] enterprise goals as an experienced and active cyber security professional practitioner and a skilled technologist.

### **Responsibilities:**

- Contributes to [The Edge] enterprise goals as a hands-on, experienced and active cyber security practitioner professional and a skilled technologist.
- Recruit new Cybersecurity/cloud technology talent and lead a dynamic team of cloud Cybersecurity and data protection architects, engineers and operations technologists to protect [The Edge] assets, data, brand and consumers in a cloud-first consumer-friendly operating model.
- Responsible for partnering with IT Architecture, IT Engineering, IT Software Engineering, IT Operations, DevOps and lines of business leaders and their teams to ensure that Cybersecurity data protection and analytics and reporting is available to be consumed help make data-driven decisions across [The Edge] enterprise and to ensure that our people, technologies and processes are adequately secured and monitored and meet Cybersecurity regulations at state, national and international levels.
- This role will work with a variety of data types and data storage systems in the cloud and from legacy systems to find creative and innovative ways to manage cyber-risks and to enable leaders and operational teams with data, reports, dashboards to help them make data-driven decisions. This role will need to be able to organize various data sets into structure repositories that will enable automated analysis that can populated regulatory compliance reporting and metrics for the overall health and operational effectiveness of the Cybersecurity program as part of the overall risk management and compliance programs across the [The Edge] enterprise.
- This is a hands-on role where the Lead is required to have the technical skills to understand and analyze the complex data sets, logs and log types, event and event types, database schemas and data feeds to move data to/from/through the end to end analytics process.
- This role will require a Cybersecurity professional and practitioner that has the experience, confidence and technical skills to rethink routine and leverage new and innovative approaches to cyber-risk management and be able to communicate complex concepts to broad range of stakeholders and align them to the strategic and tactical actions required to execute to implementation completion to operational sustainment.

- Liaison for other corporate data analytics teams and lines of business outside of [The Edge] with Humana Inc and other external, contractors, service providers, vendors, law enforcement and vendors.
- Establish data content discovery and content / file classification and tagging solutions and operational practices that track and manage risk of data content loss/leakage or unauthorized use or access or regulated/high value data and minimize the risks of data security and/or data privacy breaches
- Partner with and support other [The Edge] technology and business leaders and teams to help them has access to actionable Cybersecurity data and analysis results that support their operations and decision-making processes in timely manner.
- Recruit new talent to build a small Cybersecurity Data Protection & Analytics over time as [The Edge] business grows
- Establishing and executing on data content inspection and file tagging/classification policies, standards and practices
- Incorporate end user behavior with data content access, flow and collaboration into Cybersecurity training and awareness program to enforce data protection compliance and acceptable use policy enforcement
- Build and maintain data structures and databases in support of Cybersecurity and cyber-operations risk management
- Aggregate, normalize and analyze various log, event and data sources into cloud storage at Microsoft and Google cloud providers and use cloud analytics technologies to create actionable Cybersecurity intelligence that help driver operational actions.
- Analyze data and enable machine learning, advanced analytics, and AI in support of Cybersecurity

## **Qualifications**

- 8+ years of experience in cyber security and/or information protection practitioner and/or leadership role
- Clear understanding of cloud data/log/event collection, storage, analysis and computing and how SaaS, PaaS and IaaS solutions can accelerate innovation and delivery, while generating operational efficiencies.
- 4 or 5 years' undergraduate degree in STEM (science, technology, engineering, mathematics) or Computer Information Sciences or related discipline or 10+ years of experience in role/field Cybersecurity profession.
- 2+ years of experience or working knowledge of HIPAA Security and HIPAA Privacy regulations and requirements or Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) or NIST Special Publication 800 series Cybersecurity standards
- 2+ years of experience in managing a team of 4 more direct reports whether full time equivalents or contractors or a combination of both.

- 3 or more years of experience in Cyber Data Protection and/or Data Leakage Prevention and/or Cyber Data Analytics

*Preferred Qualifications*

- 2+ years of experience with a public cloud platform in one or more of the following cloud environments (Google Cloud Platform, Microsoft Azure, Azure AD and Office 365, Amazon Web Services)
- Competence in creating high quality reports, dashboards, graphs and metrics summary / tracking tools and visually stimulating and effective/useful displays.
- Proficient in the use of cloud native technologies, cloud Cybersecurity, and implementation patterns to lower costs, improve speed to market, increase efficiency, and enable innovation.
- A passion for simplifying and automating workflows, for making complex things easy and efficient, constantly finding new uses for data and turning data into usable information, insights and actions.
- Proficient at articulating key messages effectively, and guiding IT leaders and business partners on key concepts and strategies for enabling technology innovation.
- Experience with one or more from Microsoft Sentinel, Google Backstory, Splunk, Q-Radar, Logrhythm, Microsoft Cloud Application Security, Google Big Table, Relational Database Management Solutions, Columnar Databases, Mongo DB, Oracle DB, SQL, No-SQL, or similar Security Information & Event Management solutions..
- MBA or Master's in Comp. Sci. or MIS or Data Scientist
- Academic or practical experience background in mathematics and statistics
- Healthcare domain experience including delivering products or solutions for payers, providers, pharmacy or medical equipment and/or consumer solutions
- Cybersecurity professional certification as CISSP, CISSMP, CISSAP or CISSPE or equivalent
- Experience or background in ITL and/or Six Sigma standards and quality control disciplines
- Professional Certifications in public cloud technologies and/or solution architecture as GCP and/or Azure Architecture or Cybersecurity certifications, Kubernetes or other cloud technology specific certifications.
- Certification or qualifications in data analytics, data engineering, data scientist or similar.
- Experience working and/or managing within an environment with a "startup" culture using

**For more Information / To Apply:**

[https://humana.wd5.myworkdayjobs.com/en-US/Humana\\_External\\_Career\\_Site/job/Louisville-KY/Lead-of-Cybersecurity-Data-Protection---Analytics\\_R-232332-1](https://humana.wd5.myworkdayjobs.com/en-US/Humana_External_Career_Site/job/Louisville-KY/Lead-of-Cybersecurity-Data-Protection---Analytics_R-232332-1)