

# ALAN BERRY

**CISO**  
**CENTENE CORPORATION**

**HEADQUARTERS:** ST. LOUIS, MO

**EMPLOYEES:** 82,400

**REVENUE:** \$125 Billion (\$142 Billion projected for 2022)



PROFILES IN *Confidence*

Before becoming a CISO, Alan Berry spent the first 26 years of his career in the Air Force, where he worked across multiple departments and positions. His roles included the Director of Communications (CIO) for Air Forces Central, Commander of the 624th Operations Center (the command and control center for the Air Force global networks) and the Chief of Staff for Air Forces Cyber at Fort Meade in Maryland.

Although his work varied over the course of his 26 years in the Air Force, he found himself always coming back to work in cyber security related roles, positioning him well for the next phase of his career. After leaving the Air Force, Alan took on the role of Senior Director of the Disaster Recovery team at CVS Health where his work included restructuring the teams and technologies involved with disaster response.

After leaving CVS in 2017, Alan began working at Centene Corporation, the largest Medicaid managed care organization in the country. Centene provides a portfolio of services to government sponsored healthcare programs. He was initially hired as Vice President of Cyber Security and after three years transitioned into the CISO role.

Alan explains, "I was originally hired to lead all security operations, crisis management and business continuity. At the time we didn't have a CISO, and the job had been divided up into three people, me being one of them, but two years ago we decided to move back to having one traditional CISO role, which combined all of those responsibilities back into one office under one person."

Joining Centene was an easy choice for Alan because he believes in the organization's core mission. When he worked in the Air Force, Alan's job was to protect and defend whatever mission he was responsible for, ranging from space operations to transportation, refueling, and

combat missions across the globe. He was committed to defending these areas from a cyber perspective so adversaries could not impede the ability to conduct the missions. Alan explains, "It's the same thing a CISO does, and it's very easy to protect honorable missions. Centene works in government healthcare, providing healthcare to people who wouldn't otherwise be insured. Our mission is to transform the health of the community one person at a time. It's easy for me to get up every morning and commit to helping Centene's mission."

## CORE RESPONSIBILITIES AS CISO

Alan's responsibilities include all security operations, and incident response including threat intelligence, adversary hunting teams, and detection engineering. He oversees all systems that support these areas such as firewall proxies, vulnerability management scanners, email security systems and other key functions. His team also owns the identity process from ensuring new employees are properly entitled to managing single sign on, multifactor authentication, and everything in between.

---

**"Our mission is to transform the health of the community one person at a time. It's easy for me to get up every morning and commit to helping Centene's mission."**

---

They also manage cloud transformation as it relates to security.

As the organization continues to transition to the cloud, Alan and his team ensure security is top of mind and transforming at the same pace as the business. Alan comments, "I'm focused on increasing cyber resiliency in this cloud transition process. Moving security tools to true cloud platforms, and still performing the same functions should gain resiliency out of that. But if we don't go into it with purposeful intent, then we likely won't improve anything. There is a lot of focus to make sure what is moved to the cloud actually gains resiliency."

## COMMUNICATING EFFECTIVELY AND PROACTIVELY

Alan's tenure in the Air Force prepared him to focus on communicating effectively and proactively with executives and the board. While in the Air Force, he had to translate between mission owners like pilots, and the technical team working to fulfill the mission itself. He says, "I had to learn how to speak like a pilot or mission owner and translate the work I was doing into their language. Translating operational imperatives in the military world is no different than doing so in the corporate world. It is the same thing in a government-specific medical insurance organization, there is very specific language used on a daily basis and I have to be able to speak the language of the business to be successful."

By speaking the nuanced language of the industry Alan works in, he is able to both partner with the business and translate anything back to his team to take action on. This positions him for success, as he avoids siloes and focuses on continually unifying security with business priorities.

He explains, "For the security industry, ten years ago it was a different story with security and the business. It has improved significantly. As executives have learned more about the business of security, they have gained an appreciation for the value security brings, and discussions have become easier for security leaders. Especially as boards see incidents and other newsworthy security events happening at peer organizations. Today, most executives are invested in what security is doing and believe in what we all do enough to help us do it even better."

## AN INTENTIONAL APPROACH TO TEAM LEADING

Alan has adopted what he calls an intentional manner when communicating. He comments, "I can be very directive in how I communicate, so it's important for me to consult with

team members instead of deciding actions for them. I don't want to download the answer for anyone, I have learned to intentionally stop myself and ask them their thoughts. I enjoy when my team builds their own answer or response, and I am able to represent it for them."

When dealing with conflicting opinions, Alan relies on guiding team members through the issue by clearly laying out the pros and cons. Instead of trying to prove a case, Alan believes in taking a step back and thinking through the other person's approach and thought process. By identifying the driver of the other person's position, Alan better understands how to communicate and resolve any issues.

Alan also strongly believes in education for his team. He comments, "We have made an overt effort to focus on our internal employees' careers and education. We use NIST's National Initiative for Cybersecurity Education (NICE) framework which clearly spells out roles in cyber. We took all of these roles and turned them into Centene roles. We put in preferred education around those roles, including any certifications or additional education that is desired. This way, teammates can look at the career ladder and understand their options for growth. It helps them prepare for roles they want to grow into, and what education they might need to get there."

## API SECURITY, GOING PASSWORDLESS AND CLEARING THE ZERO TRUST NOISE

When looking ahead in the cyber industry, Alan says understanding API security will be critical for security leaders. With more systems, platforms and vendors in the cloud space, and data being exchanged in real time through APIs, security professionals must retain a strong knowledge of how this works and the impact to their programs.

Another area of focus for the industry is going passwordless. Alan believes it will transition to more mainstream and eventually become a common approach for many organizations as the complexity of passwords increases.

The other trend Alan has noticed is that organizations are moving past the buzzword filled Zero Trust marketplace. He says, "We can finally get down to the brass tacks of what companies can do in the Zero Trust space. It has been a challenge in previous years and sometimes the noise is hard to get through to understand what Zero Trust means for your organization."