

التلاعب ببيانات تكوين الشبكة: قد تؤدي السياسات غير الملائمة في إدارة وحماية بيانات التكوين الحرجة إلى سلوك غير متوقع للنظام ووصول غير مصرح به إلى منصات حيوية، مما يؤثر على سرية الشبكة وسلامتها. يتضمن هذا التهديد تعريض عنصر ووظيفة الإدارة والتنسيق للاختراق من خلال تزوير بيانات التكوين لشن هجمات SDN، أساسية في الشبكة (مثل وحدة تحكم أخرى (مثل هجمات الحرمان من الخدمة). وبينما قد يتعلق تزوير بيانات التكوين، بالبيانات التي يحتفظ بها أي مكون من مكونات الشبكة، فإن هذا التهديد يشير تحديداً إلى بيانات التكوين و/أو مستوى التحكم. فيما يلي أمثلة على التلاعب ببيانات التكوين: تزوير الإغراق الخبيث لمكونات الشبكة الأساسية: يتضمن هذا التهديد إغراق (DNS) بيانات التكوين التلاعب بنظام أسماء النطاقات أحد مكونات الشبكة بالطلبات أو حركة البيانات، مما يؤدي إلى استنفاد موارد المكون، ويؤدي إلى انخفاض أو إيقاف الخدمة التي يقدمها المكون تماماً. يتناول هذا التهديد أيضاً تقنيات أخرى، مثل التضخيم والتشبع الموصوفين أدناه. تحدث هجمات قد تأتي هجمات الإغراق على غرار هجمات الحرمان من الخدمة الموزعة، SDN التضخيم والإغراق في مكونات محددة لشبكات حيث قد يتم تنظيم عدد كبير من المصادر لتوليد سيل من الرسائل. قد تكون هذه المصادر، على سبيل المثال، أعضاء في شبكة، بوت نت