ThreatConnect Inc. lance ThreatConnect 6.4 pour améliorer les fonctionnalités de renseignements sur les menaces et les opérations de sécurité

ThreatConnect Inc.®, le leader de la sécurité axée sur les risques et les renseignements, annonce le lancement de ThreatConnect 6.4, qui intègre de nouvelles fonctionnalités permettant aux analystes des opérations de sécurité et des renseignements sur les cybermenaces (CTI, pour cyber threat intelligence) pour obtenir plus rapidement un contexte utile lors des enquêtes et améliorer l'évaluation de l'efficacité des équipes.

ThreatConnect combine sa plateforme de renseignements sur les menaces (TIP, pour Threat Intelligence Platform) et sa plateforme d'organisation et d'automatisation de la sécurité (SOAR) pour créer une boucle de rétroaction continue qui contribue à faire des opérations basées sur les renseignements une réalité. Cette dernière version du produit, qui s'appuie sur les opérations basées sur les renseignements, dynamise le flux de travail de l'équipe de renseignement et de celle des opérations de sécurité, individuellement et ensemble.

La version 6.4 offre aux équipes des CTI et du centre des opérations de sécurité (SOC, pour security operations center) un contexte plus vaste permettant aux deux équipes d'effectuer plus rapidement leurs enquêtes. Les équipes CTI peuvent créer et maintenir plus facilement une bibliothèque de menaces dynamique, et des tableaux de bord actualisés permettent aux responsables SOC et IR d'améliorer l'efficacité de l'équipe. Trois nouvelles fonctionnalités renforcent ces capacités:

- **Explore With CAL™** , pour mieux comprendre les relations complexes entre les indicateurs de menace grâce à une interface graphique intégrée à notre couche d'analyse collective
- **Browser Extension V2** , pour créer rapidement un contexte autour des menaces et améliorer votre bibliothèque de menaces
- **New Workflow Metrics**, pour améliorer l'efficacité opérationnelle en aidant les équipes SOC à apprendre comment optimiser leurs outils, leurs processus d'équipe et leurs automatisations

«Le lancement de ThreatConnect 6.4 concrétise notre vision et fournira aux équipes des opérations de sécurité et de renseignement sur les cybermenaces des capacités qui leur permettront de prendre des décisions plus rapidement dans un contexte plus pertinent, a déclaré Andy Pendergast, cofondateur et vice-président exécutif Produits de ThreatConnect. Grâce à cette nouvelle version, les équipes pourront repérer et localiser plus rapidement les menaces pesant sur leur environnement au moyen des renseignements fournis par ThreatConnect 6.4, puis décider et agir à grande échelle grâce à nos solides capacités d'organisation et d'automatisation.»

Explore With CAL™

L'architecture innovante de la couche d'analyse collective (CAL™, pour Collective Analytics Layer) de ThreatConnect relève des milliards de points de données fournissant des informations immédiates sur la nature, la prévalence et la pertinence d'une menace. La CAL offre un contexte global qui exploite les informations partagées anonymement par les utilisateurs de ThreatConnect, des informations open source, des informations sur les logiciels malveillants et de nombreuses autres séries de données.

Lorsqu'ils effectuent des recherches et des enquêtes sur une menace particulière, cette nouvelle fonctionnalité permet aux analystes de passer directement du contexte de données CAL™ à une interface graphique intuitive pour comprendre les relations et la réputation complexes existantes basées sur l'infrastructure, grâce à un indicateur spécial de compromission (IOC, pour indicator of compromise).

Browser Extension

La dernière version de la Browser Extension de ThreatConnect fait beaucoup plus que fournir des informations sur les IOC: elle permet aux utilisateurs d'analyser une ressource en ligne pour rechercher des noms d'acteurs de la menace potentielle et leurs outils. Les utilisateurs obtiennent ainsi une précieuse «pierre de Rosette» compatible CAL™ pour apparier les alias courants d'acteurs de la menace et les renseignements sur l'entité, quel que soit le nom utilisé.

Lorsqu'ils effectuent des recherches et des enquêtes sur une menace particulière, les analystes peuvent désormais utiliser plusieurs sources de renseignements sur les menaces pour repérer des éléments d'information pertinents à partir de n'importe quelle ressource Web. Cette fonctionnalité est essentielle lorsqu'il s'agit de comprendre rapidement le niveau de gravité de la menace et permet aux utilisateurs de l'ajouter à leur bibliothèque de menaces pour leurs futurs efforts d'analyse et d'enquête.

Workflow Metrics

Workflow metrics amplifie la visibilité de vos opérations de sécurité grâce à des indicateurs de performance clés essentiels qui mesurent si les personnes, les outils et les technologies travaillent ensemble efficacement. La version 6.4 améliore l'évaluation des flux de travail en fournissant des informations plus précises sur les tendances de la détection et des réponses au cours d'une période déterminée. Les responsables des équipe SOC disposent également d'une perspective sur la répartition des cas entre équipes, ainsi que sur la meilleure façon de hiérarchiser les cas non affectés.

Un tableau de bord indiquant le temps moyen de détection (MTTD, pour Mean Time to Detection) et le temps moyen de réponse (MTTR) sur des périodes de temps variables a été ajouté pour aider les responsables SOC à évaluer les tendances en matière de détection et de réponse. De nouvelles cartes de tableau de bord simples à configurer pour les cas actifs et non attribués permettent aux responsables d'équipe de prendre des décisions plus éclairées lors de la gestion de la charge de travail des équipes.

Axée sur le risque et les renseignements, l'approche de ThreatConnect réduit la complexité en

intégrant les processus et les technologies pour renforcer continuellement les défenses, atténuer les risques et révolutionner la façon dont les clients protègent leurs organisations en transformant les renseignements en action.

À propos de ThreatConnect

ThreatConnect Inc. fournit un logiciel de cybersécurité qui simplifie le travail de tous, facilite la prise de décision en transformant les informations en action, et intègre les processus et les technologies pour renforcer les défenses et atténuer les risques en permanence. Conçue par des analystes, mais élaborée pour l'ensemble de l'équipe (leadership en matière de sécurité, risques, opérations de sécurité, renseignements sur les menaces et réponse aux incidents), la plateforme d'aide à la décision et d'appui opérationnel de ThreatConnect est actuellement la seule solution disponible réunissant la quantification des cyberrisques, les informations sur les cyberrisques, l'automatisation et l'analyse des cyberrisques et les flux de travail liés aux cyberrisques. Pour en savoir plus sur nos solutions de quantification des cyberrisques (CRQ, pour Cyber Risk Quantification), de plateforme de renseignements sur les menaces (TIP, pour Threat Intelligence Platform) ou d'organisation, d'automatisation et de réponse de sécurité (SOAR, pour Security Orchestration, Automation and Response), rendez-vous sur www.ThreatConnect.com.

Le texte du communiqué issu d'une traduction ne doit d'aucune manière être considéré comme officiel. La seule version du communiqué qui fasse foi est celle du communiqué dans sa langue d'origine. La traduction devra toujours être confrontée au texte source, qui fera jurisprudence.

Consultez la version source sur businesswire.com : https://www.businesswire.com/news/home/20211129005695/fr/