NOTE DE SYNTHÈSE

# THREAT INTELLIGENCE DATA EXCHANGE (TIDE)

## Optimisez l'efficacité des SecOps grâce à la gestion et à l'automatisation de la threat intelligence

### L'EFFICACITÉ DE LA SÉCURITÉ DÉPEND D'UNE THREAT INTELLIGENCE (TI) DIVERSIFIÉE ET PRÉCISE

Pendant des décennies, la plupart des entreprises les plus importantes et les plus sécurisées au monde ont adopté une approche de sécurité « multi-fournisseurs », convaincues qu'aucun fournisseur unique ne pouvait fournir suffisamment de threat intelligence pour les protéger contre un environnement de menaces en constante évolution. Ainsi, elles orchestre leurs défenses pour forcer les attaques à travers plusieurs solutions, provenant de différents fournisseurs, espérant qu'au moins l'un de ces fournisseurs disposerait de la threat intelligence nécessaire pour détecter une partie de l'attaque tout au long de la kill chain.

Ces dernières années, des études ont confirmé la valeur de cette approche en révélant le faible recoupement entre les flux de threat intelligence issus de fournisseurs, de sources open source, de la communauté et d'autres canaux. Dans une étude, une comparaison des données de threat intelligence fournies par deux fournisseurs de sécurité n'a révélé qu'un recoupement de 11 %, ce qui signifie que 89 % des données de chaque fournisseur étaient uniques.

Cela a conduit à la recherche d'une solution optimale combinant plusieurs sources de threat intelligence afin d'aider les entreprises à tirer le meilleur parti de leur investissement global en matière de sécurité. Malheureusement, cet effort a alourdi la charge de travail des équipes SecOps, qui doivent désormais identifier, collecter, normaliser et distribuer différents types de threat intelligence provenant de dizaines de sources disponibles, puis fournir la bonne combinaison de TI à chaque outil de sécurité. La plupart se retrouvent ainsi à jongler avec un mélange d'outils commerciaux et de solutions maison, reliés par des API, des scripts et des macros, dans l'espoir d'obtenir un minimum d'efficacité.

### INFOBLOX TIDE SIMPLIFIE LES EFFORTS D'OPTIMISATION DE LA TI

Infoblox BloxOne Threat Defense Advanced offre une fonctionnalité permettant de rationaliser la collecte et la gestion de la threat intelligence, appelée TIDE (Threat Intelligence Data Exchange). En plus des 30 flux de menaces inclus dans BloxOne Threat Defense, TIDE offre la possibilité d'intégrer la Threat Intelligence provenant d'autres sources et de contrôler la manière dont ces informations sont distribuées dans la pile de sécurité afin de rendre chaque outil aussi efficace que possible.

### DES FAITS ET DES CHIFFRES

Selon l'enquête 2021 de SANS Cyber Security Intelligence (CTI) :

- **2/3 des répondants ont des difficultés** à distribuer les informations CTI par e-mail ou dans des documents
- Plus de la moitié des répondants citent **le manque de personnel, de compétences ou de financement** comme des obstacles à l'efficacité de la CTI
- Les auteurs de l'enquête SANS concluent que **l'automatisation est nécessaire pour soutenir l'efficacité et l'ampleur de la CTI**

**Les principaux avantages de TIDE incluent :**

- La collecte et la gestion en temps réel de threat intelligence issue de multiples sources, au sein d'une plateforme unique, ouverte et flexible
- Une assistance pour accélérer les enquêtes et les réponses aux menaces grâce à plus de 300 domaines de classification des menaces distincts
- Une amélioration de l'efficacité des SecOps et de l'ensemble de la pile de sécurité grâce à une threat intelligence facile à partager
- La détection et le contrôle des activités malveillantes hautement évasives au niveau de la couche DNS, car cette même threat intelligence est appliquée par BloxOne
- Threat Defense pour révéler les risques tels que les portes dérobées, les communications C2, le tunneling ou l'exfiltration de données via DNS

TIDE d'Infoblox est conçu pour maintenir à jour en temps réel les systèmes de sécurité tels qu'Infoblox BloxOne Threat Defense et le reste de l'écosystème de cybersécurité contre les menaces nouvelles et en constante évolution. Combinez jusqu'à 30 sources de threat intelligence différentes fournies par Infoblox avec toutes les autres sources disponibles dans le commerce, provenant de sources gouvernementales ou industrielles, open source ou de vos propres ensembles de données TI internes. Grâce à ses capacités d'automatisation et à la prise en charge de nombreux formats de fichiers, TIDE permet aux clients de collecter et de diffuser les données pertinentes de threat intelligence vers l'ensemble de leur écosystème : pare-feux, solutions SIEM, SWG, SOAR, scanners de vulnérabilités, etc.

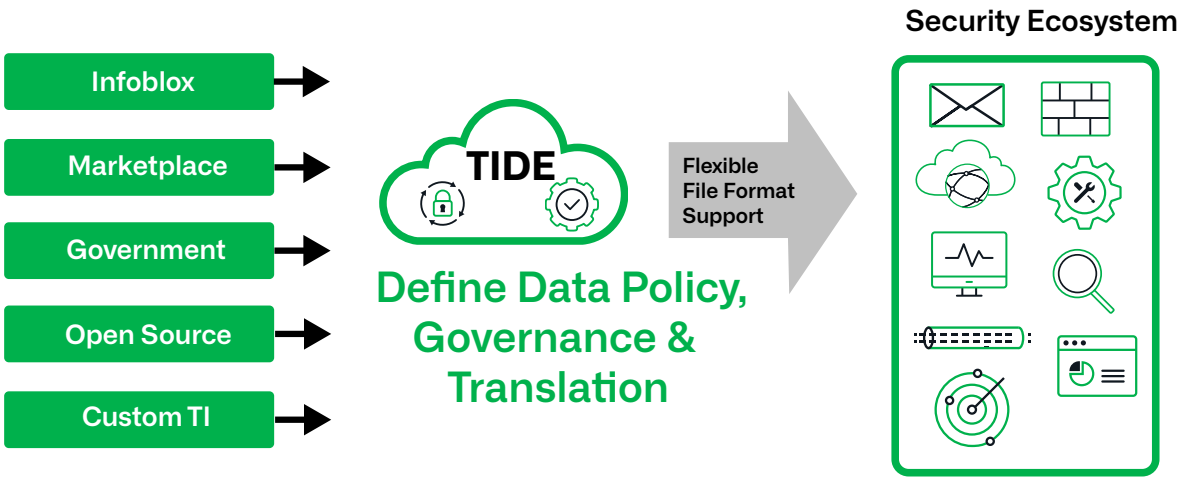


*Figure 1 : TIDE facilite l'échange de threat intelligence au sein de l'écosystème de sécurité, renforçant ainsi les défenses et améliorant les reporting.*

## L'UNE DES NOMBREUSES FONCTIONNALITÉS AVANTAGEUSES DE BLOXONE THREAT DEFENSE

TIDE est l'une des nombreuses fonctionnalités qui composent BloxOne Threat Defense, une solution de sécurité cloud-native qui protège contre les malwares actuels, les ransomwares, les communications C&C, l'exfiltration de données et d'autres menaces avancées en utilisant le DNS comme première ligne de défense. Elle comprend des fonctionnalités qui améliorent l'ensemble de la pile de sécurité et rendent les opérations de sécurité plus efficaces, notamment en leur permettant de mener plus rapidement des enquêtes sur les menaces et d'y répondre plus rapidement et avec une plus grande confiance. Il s'agit de la première solution de sécurité du secteur pour notre réalité hybride moderne qui offre une protection omniprésente partout pour tous les appareils du réseau, y compris les appareils BYOD et IOT/OT.

## OPTIMISEZ LA RECHERCHE, L'INVESTIGATION ET LA RÉPONSE AUX MENACES

BloxOne Threat Defense Advanced offre une autre fonctionnalité qui permet aux analystes d'accéder à l'ensemble des informations de threat intelligence et de les exploiter dans une vue unique appelée Dossier. Dossier fournit un accès à la demande à la sévérité des menaces, aux données WHOIS, aux conseils

MITRE ATT&CK, à des extraits de fichiers, aux adresses IP/URL/domaines associés, aux informations sur les cybercriminels, aux chronologies des activités, et bien plus encore. Il permet aux analystes de se concentrer sur ce qui est important, en s'appuyant sur les données et leur expérience, afin de parvenir plus rapidement à des conclusions fiables.

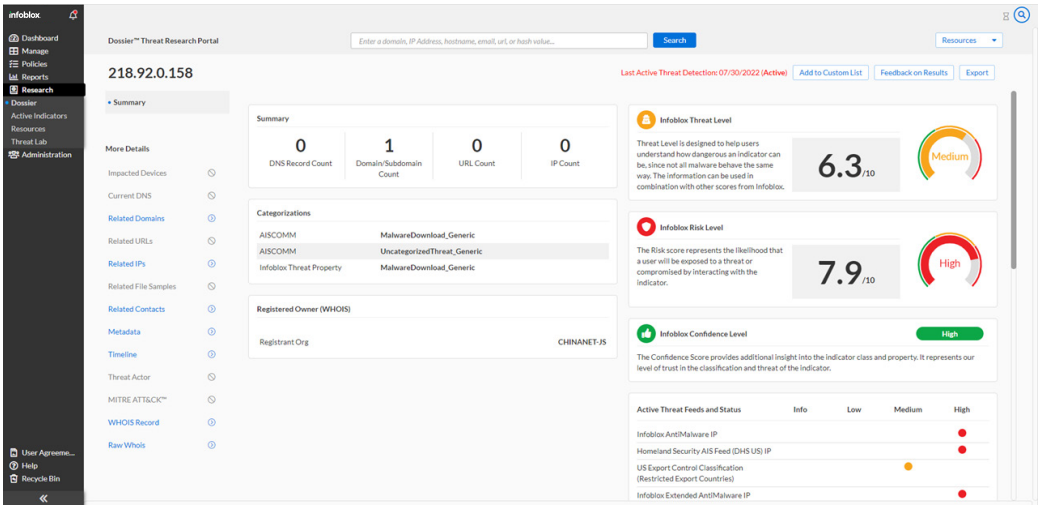


*Figure 2 : le tableau de bord Dossier vous permet d'approfondir et de modifier vos analyses à tout moment.*

## INTÉGRATIONS PRÊTES À L'EMPLOI : FLUX DE THREAT INTELLIGENCE TIERS

Bien que la fonctionnalité TIDE de BloxOne Threat Defense permette de simplifier et d'automatiser l'intégration de la plupart des flux de threat intelligence et leur distribution vers quasiment tous les outils de sécurité, certains partenaires ont collaboré avec Infoblox pour en faciliter davantage l'intégration côté client.

Les partenaires suivants offrent une assistance prête à l'emploi pour la fonctionnalité TIDE :

**CrowdStrike :** CrowdStrike est un fournisseur de premier plan de protection des endpoints de nouvelle génération, de threat intelligence et de services. Les informations sur les noms d'hôte et les adresses IP fournies par CrowdStrike Falcon permettent aux clients de prévenir les préjudices causés par les attaques ciblées, de détecter et d'attribuer les malwares avancés et les activités malveillantes en temps réel, et de rechercher facilement tous les endpoints, réduisant ainsi le temps global de réponse aux incidents. Les clients doivent acheter le flux CrowdStrike directement auprès de CrowdStrike, mais Infoblox peut vous aider à « activer » le flux dans la plateforme TIDE.

**FireEye iSight Threat Intelligence :** son adresse IP et son nom d'hôte fournissent aux entreprises des analyses stratégiques, opérationnelles et tactiques issues de son équipe mondiale d'experts. Un abonnement à ThreatScape fournit les informations nécessaires pour aligner un programme de sécurité sur les objectifs de gestion des risques de l'entreprise et pour se défendre de manière proactive contre les cybermenaces nouvelles et émergentes. Bien que les clients doivent acheter le flux iSight directement auprès de FireEye, Infoblox peut aider à « activer » le flux sur la plateforme TIDE.

En outre, les abonnés à BloxOne Threat Defense Advanced peuvent tirer parti des flux des fournisseurs tiers suivants (abonnement supplémentaire requis) au format RPZ (sans frais supplémentaires) pour augmenter leur couverture des menaces au niveau du plan de contrôle DNS :

**Farsight Security Newly Observed Domains (NOD) Feed :** ce flux offre une protection supplémentaire contre l'exfiltration de données par les malwares, le détournement de marque et les attaques par spam ayant pour origine ou pour destination des domaines nouvellement lancés.

**Flux de réputation des adresses IP et des domaines Proofpoint Emerging Threats (ET) :** ce flux fournit des informations exploitables sur la réputation des adresses IP et des domaines, qui sont notées en fonction des observations du comportement des cybercriminels en situation réelle et des observations directes des laboratoires ET Labs de Proofpoint. S'appuyant sur un processus propriétaire qui exploite l'un des plus grands réseaux d'échange de malwares actifs au monde, une émulation à grande échelle des victimes, une technologie de détection unique et un réseau mondial d'outils de surveillance, Proofpoint ET Intelligence est mis à jour en temps réel afin de fournir aux entreprises des informations exploitables pour lutter contre les menaces émergentes actuelles.



**Siège social**
2390 Mission College Boulevard, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com



Version : 20231030v1