CALID
CENTRE D'ANALYSE EN LUTTE
INFORMATIQUE DÉFENSIVE

DGA

DÉTECTION D'ANOMALIES POUR L'AIDE AU HUNTING

C&ESAR 2018

DGA
CALID
CENTRE D'ANALYSE EN LUTTE
INFORMATIQUE DÉFENSIVE

Contexte

- Activité de hunting
- Grande quantité de journaux applicatifs

Objectifs

- Aider l'analyste pour prioriser les investigations
- Déterminer les éléments les plus anormaux dans la population
- Donner les raisons de la suspicion

Méthodologie

- Analyse des formats de log disponibles
- Définition des Entités à qualifier
  - Machines, utilisateurs, flux, ...
  - ... sur une période temporelle
- Caractérisation de ces Entités
  - Métriques calculées par entité et par période
- Identification des anomalies
  - vecteurs de métriques = entrée des algorithmes d'apprentissage

Cas d'usage

- Format = journaux de proxy d'accès à Internet
- Entité = machine interne identifiée par son adresse IP
- Période temporelle = 6h
- Algorithmes = Auto-encodeur et Forêt d'isolation
- Métriques = > 30

Exemples de métriques

- Nombre de connexions HTTP utilisant la méthode POST
- Nombre de pics de connexions HTTP utilisant la méthode POST
- Nombre d'octets échangés
- Nombre de pics d'octets échangés
- Nombre de connexions pour laquelle l'URL a une longueur relativement grande ou basse
- Nombre de requêtes vers des domaines sur liste noire
- Nombre de chaînes user-agents différentes

Principe

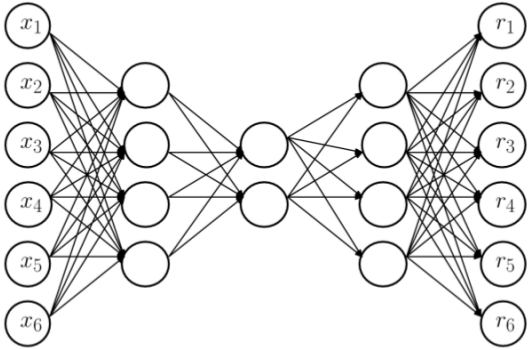
- Algorithmes de détection d'anomalies non-supervisés
  - Calcul d'un score d'anomalie pour chaque entité par période temporelle
- Combinaison des scores d'anomalies de chaque algorithme
  - Obtention d'un score global
- Présentation des entités par score décroissant

Algorithmes utilisés

- Auto-encodeur
  - Réseau de neurones
- Forêt d'isolation
  - Algorithme de partitionnement

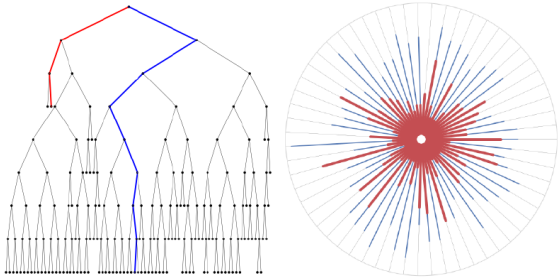
Auto-encodeur

- Apprentissage d'une fonction d'identité
- Fonction de transfert ReLu
- Score d'anormalité = erreur de reconstruction

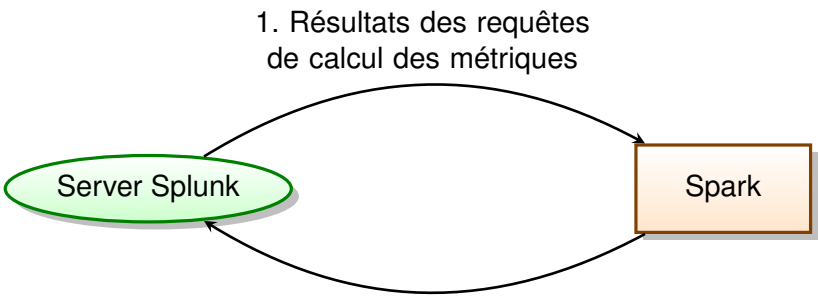


Forêt d'isolation

- Hypothèse : les anomalies sont rares et différentes
- Construction d'arbres binaires aléatoires
- Les anomalies ont une plus forte probabilité d'être isolées rapidement
- Leur distance à la racine de l'arbre est plus faible



Architecture



Performances à évaluer

- Temps de calcul
- Détection de comportements malveillants
- Analyse des faux positifs

Temps de calcul

- Performances de calcul raisonnables
  - Calcul des métriques : 15min
  - Calcul des scores : 10min

Performances de détection

- Comment maîtriser le nombre de faux négatifs ?
- En contrôlant les comportements malveillants présents
  - Injection de traces synthétiques de comportements malveillants
  - Maîtrise des valeurs de champs et de l'aspect temporel
  - 9 scénarios malveillants générés

Scénarios générés

- Activités d'un malware
  - Téléchargements initiaux
  - Contact de serveurs C&C
- Communications avec des domaines DGA
- Saturation d'un serveur externe
  - POST Flood
  - Téléchargement répétitif
- Exfiltration de données
  - via un domaine unique
  - via des domaines DGA
  - via un service WEB connu

Résultats

- Hypothèse : Seulement 5 entités peuvent être analysées par période

Comportement malveillant	Visible pour l'analyste	Meilleur rang (Moyenne)	Rang de référence (Moyenne)
coms-dga	✓	1,6	7004
url-exfilt	✓	2,3	14933
post-flood	✓	2,7	1612
dga-exfilt	✓	2,8	10288
post-flood-2	✓	3,5	22194
pdf-downl	✓	3,6	11588
url-exfilt-2	✗	13,8	6712
malw-cc	✗	28,6	10214
fb-exfilt	✗	406,7	15990

Tableau de bord

[ML] TOP 50 des adresses IP anormales

Modifier | Exporter | ...

Période: Les 2 derniers mois

Date: 2018-08-13

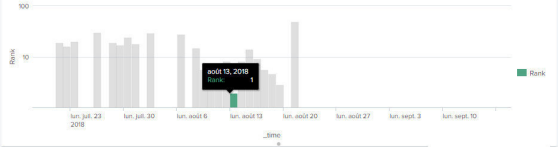
Masquer les filtres

Top 50

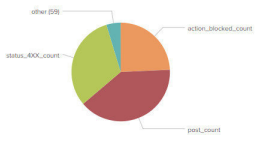
Date	Position	Adresse IP	investiguer	iforest_anomalyProbability	iforest_score	rnn_anomalyProbability	rnn_score
2018-08-13	1	[redacted]	GO	0.5296	0.588347368800287	1.0000	350.07038899408116
2018-08-13	2	[redacted]	GO	0.5219	0.5850121636276745	0.6680	233.84211322653726
2018-08-13	3	[redacted]	GO	0.7717	0.6936883149880047	0.5642	197.5095508635987
2018-08-13	4	[redacted]	GO	0.8538	0.7293645902851391	0.5610	196.41547534276535
2018-08-13	5	[redacted]	GO	0.9692	0.7755926307895891	0.5580	195.34062268377411
2018-08-13	6	[redacted]	GO	0.3558	0.5127693797459059	0.5073	177.59108526601096
2018-08-13	7	[redacted]	GO	0.9826	0.7854163540498413	0.4888	171.1429972725899
2018-08-13	8	[redacted]	GO	0.7485	0.6835832742538677	0.4673	163.6106336486864
2018-08-13	9	[redacted]	GO	0.3860	0.525881016984978	0.4648	162.72310966294077
2018-08-13	10	[redacted]	GO	0.9609	0.7755561906785513	0.4320	151.2468212857478

« préc 1 2 3 4 5 suiv »

Rang sur la période



Feature contribution



Quelques faux positifs expliqués

Métrique explicative	Comportement anormal constaté
Nombre de type "video" élevé	Onglet resté ouvert la nuit avec un flux vidéo en boucle.
Taux d'exceptions élevé	Synchronisation de boîte mail externe avec un problème d'authentification
Nombre de "POST" de type "application"	Participation à une conférence sur plusieurs jours

Synthèse

- Expérimentation d'algorithmes de détection d'anomalies pour l'aide au Hunting
- Les anomalies et comportements anormaux bruyants sont détectés

Perspectives

- Injection de comportements malveillants plus fins
- Modification des hyper-paramètres
- Autres algorithmes (KNN)

- Active learning
  - Association avec un classifieur supervisé ([AI2])
  - Active Anomaly Discovery
- Sélection des métriques
  - Génération de règles pour aider l'analyste
- Série temporelle
  - Approche minimaliste
  - Détection d'anomalies dans la dynamique temporelle