Alertes basées sur le risque

Reprendre le contrôle des opérations

Améliorer l’efficacité de votre centre des opérations de cybersécurité (SOC) et augmenter le bonheur de vos analystes.

Jean-François Brouillette

Fondateur de Cyber Formation Québec

Chef de pratique IR – Banque Nationale du Canada

- Administrateur de systèmes et développement Web/applicatif
- Conseiller en cybersécurité
- Enquêtes numériques et réponse aux cyberincidents
- Chef de pratique – Réponse aux cyberincidents

Défis d’une organisation

01

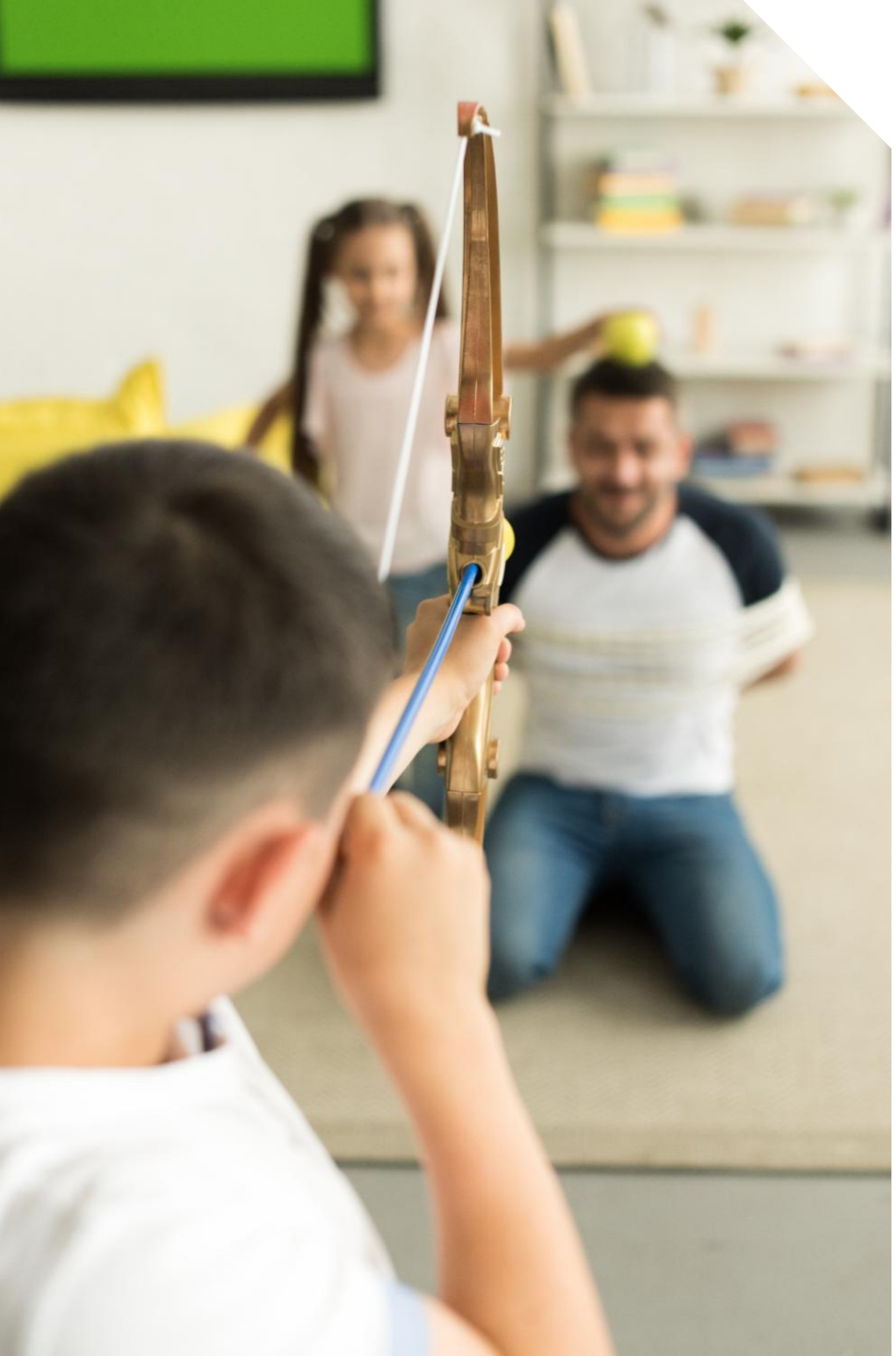
Mobilisation des analystes

Le volume des alertes à traiter et leur pertinence ont un impact direct sur l’efficacité et la mobilisation des analystes.

02

Pertinence des alertes

Le traitement à la pièce des alertes peut être dangereux et vous rendre aveugle sur une attaque sophistiquée.



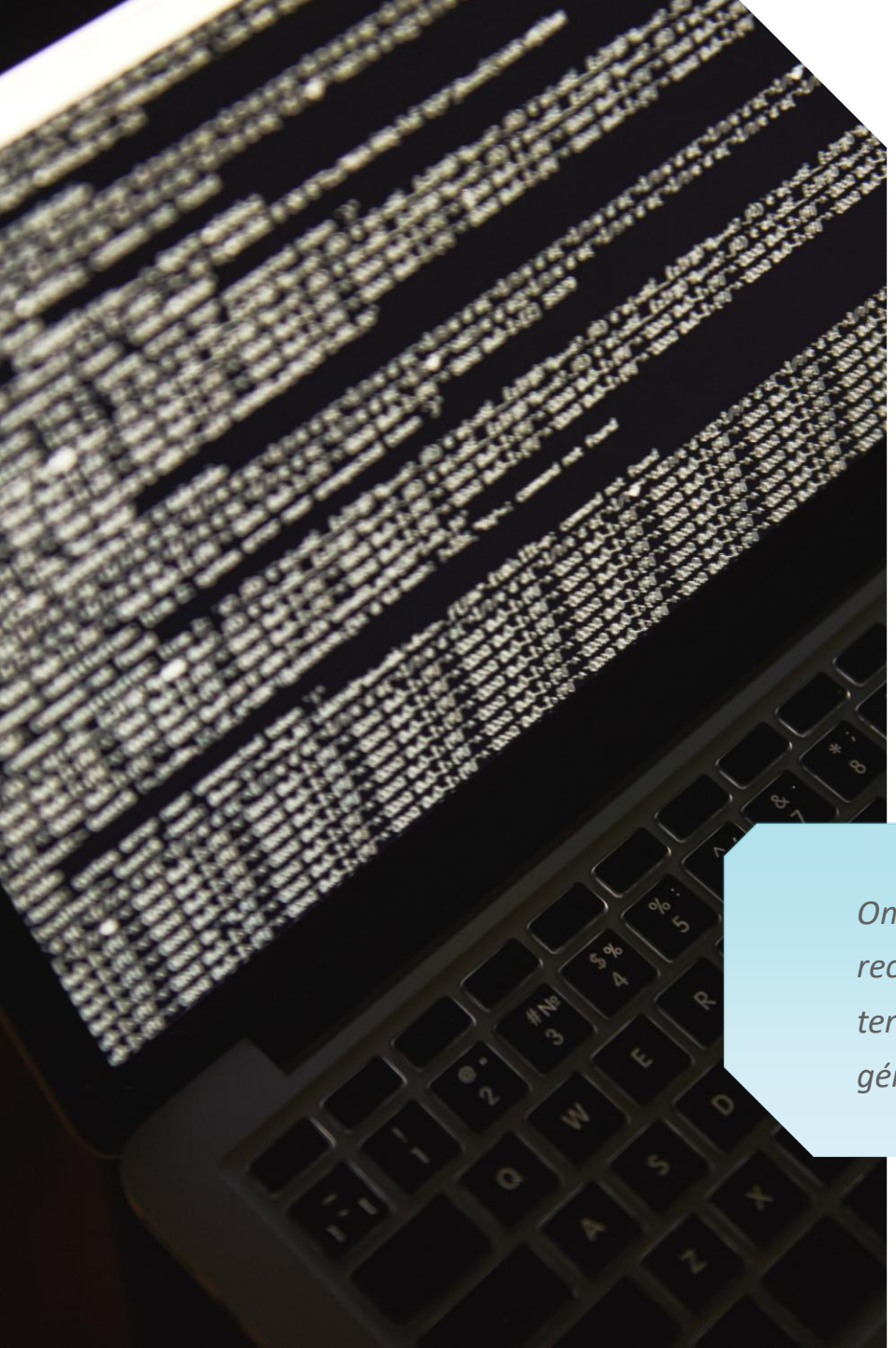
Objectifs

- Comprendre l’importance de faciliter le travail des analystes dans leur quotidien (fatigue des alertes, traitement individuel des alertes)
- Déterminer comment les alertes basées sur le risque peuvent aider à se concentrer sur les attaques ou événements qui représentent un plus grand danger pour l’organisation
- Être conscient des risques que peut comporter cette méthodologie

Des dizaines de solutions…

On reçoit maintenant des dizaines, voire centaines d'alertes via les multiples solutions de cybersécurité en place. Ceci génère un volume important qui peut vite fatiguer les analystes et rendre moins efficaces.

Malgré tous vos efforts, les comités de revue des cas d'usages (UC), l'optimisation des détections, il est possible que vous cherchiez une autre méthode pour réduire la charge de travail de votre équipe.



Raconte-moi une histoire…

Une alerte sans contexte, sans enrichissement, sans autres événements liés, ça peut laisser croire à une activité légitime.

On peut comparer les attaques menées par les acteurs malicieux à une recette de cuisine, il faudra plusieurs étapes et ingrédients pour la mener à terme. Chaque étape pourrait être vue comme des événements notables qui génèrent un score de risque.

```
Nov 7, 2022 @ 11:58:44.538   sshd: Attempt to login using a non-existent user
Nov 7, 2022 @ 11:58:44.538   sshd: Attempt to login using a non-existent user
Nov 7, 2022 @ 11:58:42.793   PAM: User login failed.
Nov 7, 2022 @ 11:58:42.753   PAM: Multiple failed logins in a small period of time.
Nov 7, 2022 @ 11:58:42.753   PAM: User login failed.
```

56
RISK

Remote Service Launch

LATERAL MOVEMENT

Sep 5 14:00
lasting an hour

[redacted] received a request from a remote client to launch a service. This is the first time [redacted] received this type of request from the remote client. Specific tools, such as PsExec, can create a temporary service that enables a remote attacker to run commands or launch executable files.

Service names linked to this detection:

- PSEXESVC

Commands linked to this detection:

- %SystemRoot%\PSEXESVC.exe

Chapitres de l’histoire

MITRE ATT&CK®

Initial Access (TA0001)

Alerte générée par l’EDR

Spearphishing Attachment

(T1566.001

par le SIEM

x d’événements Windows)

Scheduled Task (T1053.005)

Command &

Alerte g

Web Serv ectional

Communication (T1102.002)

Impact (T0040)

Alerte générée par l’EDR

Data Encrypted for Impact (T1486)

Chapitres de l’histoire

Initial Access (TA0001)

Alerte générée par l’EDR

Spearphishing Attachment (T1566.001)

Execution (TA0002)

Événement reçu par le SIEM (Journaux d’événements Windows)

Scheduled Task (T1053.005)

Command & Control (TA0011)

Alerte générée par le NDR

Web Service: Bidirectional Communication (T1102.002)

Impact (T0040)

Alerte générée par l’EDR

Data Encrypted for Impact (T1486)

Chapitres de l’histoire

Expéditeur, utilisateur, IP de l’expéditeur

Initial Access (

A

Execution (TA0002)

Événement reçu par le SIEM
(Journaux d’événements Windows)
Scheduled Task (T1053.005)

Command & Control (TA0011)

- Alerte générée par le NDR
  Web Service: Bidirectional Communication (T1102.002)

Impact (T0040)

Alerte générée par l’EDR
Data Encrypted for Impact (T1486)

Chapitres de l’histoire

Initial Access (TA0001)

Alerte générée par l’EDR

Spearphishing Attachment (T1566.001)

Execution (TA0

Évé

Windows)

1053.005)

Nom d’hôte, utilisateur, signature numérique

Command & Control (TA0011)

Alerte générée par le NDR

Web Service: Bidirectional Communication (T1102.002)

Impact (T0040)

Alerte générée par l’EDR

Data Encrypted for Impact (T1486)

Chapitres de l’histoire

Initial Access (TA0001)

Alerte générée par l’EDR

Spearphishing Attachment

(T156

NDR

Bidirectional

nication (T1102.002)

Nom d’hôte, utilisateur, IP/domaine de l’application Web

Execution (TA0002)

Événement reçu par le SIEM

(Journaux d’événements Windows)

Scheduled Task (T1053.005)

Impact (T0040)

Alerte générée par l’EDR

Data Encrypted for Impact (T1486)

Chapitres de l’histoire

Initial Access (TA0001)

Alerte générée par l’EDR

Spearphishing Attachment (T1566.001)

Execution (TA0002)

Événement reçu par le SIEM (Journaux d’événements Windows)

Scheduled Task (T1053.005)

Command & Control (TA0011)

Alerte générée par le NDR

Web Service: Bidirectional Communication (T1102.002)

Imp

DR

d for Impact (T1486)

Nom d’hôte, utilisateur

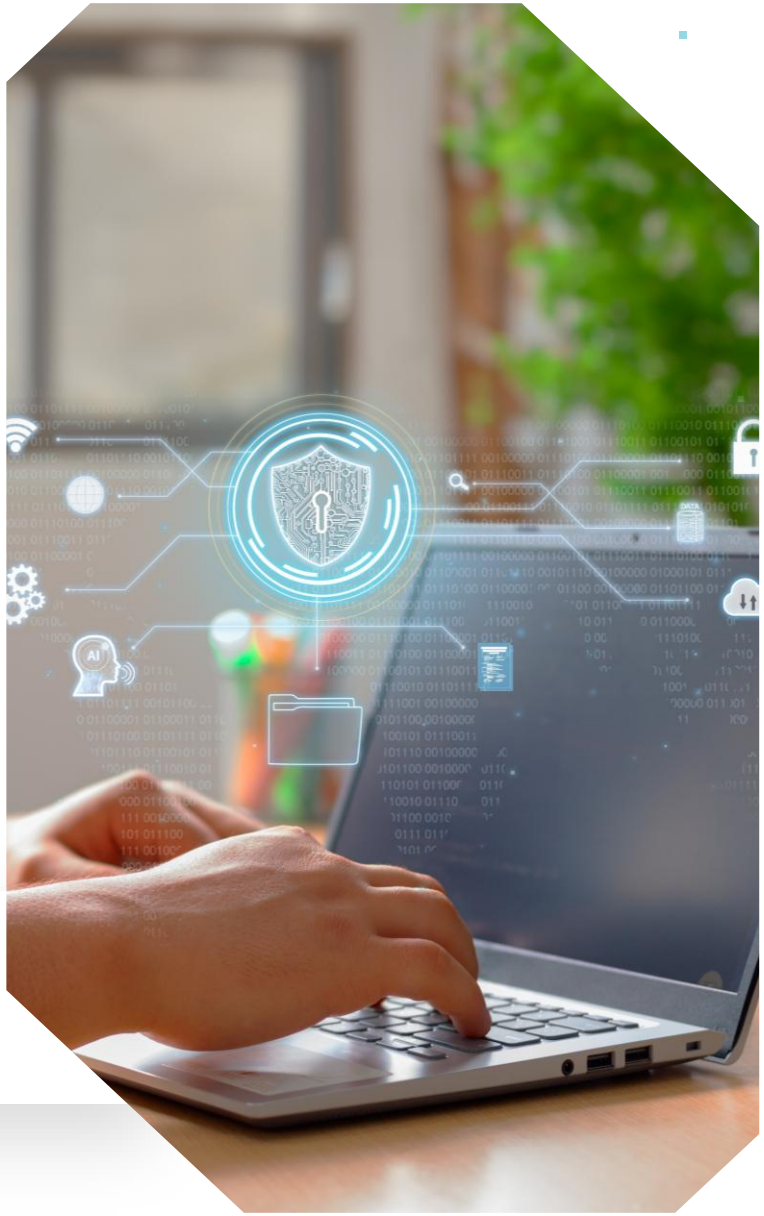
Enrichissement et contexte

Multiplicateur de risque

Afin d’être optimal dans le calcul des scores de risque, les données doivent être standardisées. De plus, plusieurs facteurs peuvent venir augmenter ou diminuer la valeur du risque attribuée.

- Cyber Threat Intelligence
- Équipe de fraude
- Menace interne

- Public-facing
- Vulnérabilités
- “Crown Jewel”



Un fil conducteur

Exemple d’objets de risque: adresse IP, nom de domaine, nom d’hôte, nom de fichier, signature numérique, etc.

Intervenir rapidement

Un analyste d’expérience sera en mesure de rapidement déterminer s’il s’agit d’événements suspects ou non.

Vue globale

Votre alerte basée sur le risque vous permet d’avoir une vue d’ensemble sur l’attaque.

Une sévérité adaptée

Une alerte basée sur le risque requiert généralement qu’on s’y attarde rapidement considérant qu’il s’agit d’une succession d’événements.

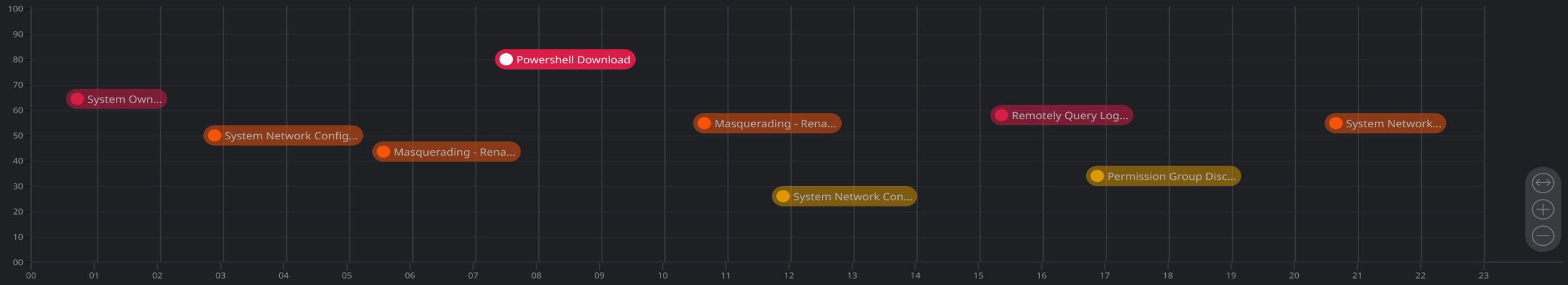
La sévérité de ces alertes pourrait être adaptée pour passer plus rapidement le triage.

Risk Events

Adam's Desktop

Aggregated Risk Score: 200 | Threshold: 150

Events in 24h: 9



Contributing Risk Events

Search

	CREATED	RISK RULE	RISK SCORE	ANNOTATIONS	THREAT OBJECT
⌄	Today, 12:50 AM	Threat - RR - Powershell Download	80	TA0005, TA0007, T1036	foo.exe + 2

Risk Object	Adam's Laptop	Threat_Object	foo.exe
Source	Threat - UEBA Anomaly Detected (Risk) - Rule	Threat_Object-Type	Executable
Calculated Risk Score	80		
Risk_Message	Detects UBA anomaly events	View Raw event	
Saved_Search_Description	Detects UBA anomaly events		

›	Thu, Mar 18 2020	Threat - RR - System Owner/User discovery	65	TA0005, TA0007, T1036	foo.exe, raw-shield... + 2
›	Thu, Mar 18 2020	Threat - RR - Remotely Query Login Sessions	70	TA0005, TA0007, T1036	foo.exe, proident_xls.ini
›	Thu, Mar 18 2020	Threat - RR - System Network Connections discovery	50	TA0005, TA0007, T1036	foo.exe, occaecatC... + 1
›	Thu, Mar 18 2020	Threat - RR - Masquerading - Renamed Binary	55	TA0005, TA0007, T1036	proident.exe, foo.exe
›	Thu, Mar 18 2020	Threat - RR - System Network Configuration discovery	55	TA0005, TA0007, T1036	readme.txt, foo.exe

À réfléchir lors de la mise en place

A

Données standardisées

Il est primordial que les événements suivent un standard dans votre SIEM

B

Délai possible

Le début d'une attaque pourrait être visible après un certain délai. (Bien définir le temps de corrélation des alertes)

C

Constance des scores

Il faut être conséquent et définir une méthodologie de calcul.

MERCI

Des questions?

https://www.linkedin.com/in/jfrancoisb/
jfb@cyberformationquebec.ca

https://cyberformationquebec.ca