Robocert : Traitement semi-automatisé des incidents sécurité grâce à des web-services

Jean Benoit, Guilhem Borghesi

Robocert : Traitement semi-automatisé des incidents sécurité grâce à des web-services

Jean BENOIT
Direction Informatique - Département Infrastructure
Université de Strasbourg
14, rue René Descartes
67 000 Strasbourg

Guilhem BORGHESI
Direction Informatique - Département Infrastructure
Université de Strasbourg
14, rue René Descartes
67 000 Strasbourg

Résumé

La Direction Informatique et le CERT Osiris traitent conjointement environ 600 incidents sécurité par an. Une telle quantité d'incidents peut difficilement faire l'objet d'un traitement manuel. La première tentative d'automatisation était un simple script qui permettait de simplifier le traitement en regroupant les différentes étapes du processus : ouverture de l'incident, collecte d'informations, analyse, blocage éventuel de l'adresse IP ou du compte concerné, suivi d'incident et clôture. Ce script faisait déjà appel à un outil de ticket et à différents référentiels. L'idée est progressivement apparue de renforcer l'automatisation du traitement en employant une représentation structurée des données de l'incident, de manière à avoir un format exploitable par un programme. En concertation avec le CERT RENATER, les notifications d'incident nous ont été transmises dans une représentation structurée au format IODEF. Pour décrire très simplement son fonctionnement, notre nouvel outil, Robocert, décode ce format et collecte un maximum d'informations pour simplifier les actions de l'opérateur qui traite les incidents. Cet article décrit les différentes représentations structurées existantes d'incidents de sécurité. Il détaille également la façon dont Robocert fonctionne et l'organisation des web-services sur lesquels il s'appuie, et enfin il envisage les évolutions possibles pour cet outil.

Mots clefs

sécurité, incident, IODEF, automatisation, CERT

1 Introduction

La Direction Informatique et le CERT Osiris traitent conjointement environ 600 incidents sécurité par an. Une telle quantité d'incidents peut difficilement faire l'objet d'un traitement manuel. Pendant plusieurs années, un simple script permettait de simplifier le traitement en regroupant les différentes étapes du processus. Ce script précédent faisait déjà appel à un outil de ticket et à différents référentiels. L'idée est progressivement apparue de renforcer l'automatisation du traitement en se basant sur une représentation structurée des données de l'incident, de manière à avoir un format exploitable par un programme. En concertation avec le

CERT RENATER, les notifications d'incident nous ont été transmises dans une représentation structurée au format IODEF [1]. Pour décrire très simplement son fonctionnement, notre nouvel outil, Robocert, décode ce format et collecte un maximum d'informations pour simplifier les actions de l'opérateur qui traite les incidents. Nous introduirons tout d'abord les différentes représentations structurées existantes d'incident sécurité, puis nous détaillerons la façon dont Robocert fonctionne, et enfin nous aborderons les évolutions envisagées pour cet outil.

2 Les formats de description et de signalisation d'incident

2.1 Les standards existants

Comme dans beaucoup de situations, il existe de nombreuses façons de modéliser ce qui est observé ; on trouve donc différents formats pour décrire un incident de sécurité dans le but d'en automatiser le traitement. Il est assez fréquent que ces formats s'appuient sur XML. Chaque format est conçu pour différents usages ; ces formats sont notamment utilisés pour :

— importer et exporter des données entre applications (entre un IDS et un système de gestion d'incidents par exemple),

— effectuer des recherches multi-critères (adresse IP, numéro de port, intervalle de dates etc) sur un ensemble d'incidents (dans le but de corréler des incidents par exemple),

— à partir des données d'incident, alimenter des dispositifs de détection ou de filtrage.

— transmettre une intention («ce fichier est une notification d'incident»), voire demander une action de la part du récepteur («merci de faire cesser ce trafic»),

Certains formats offrent de plus des fonctions de sécurité comme :

— le contrôle du partage de certaines informations sensibles (à qui ces informations peuvent-elles être données ?),

— la signature et le chiffrement des données d'incident,

IDMEF et IODEF sont sans doute les formats les plus répandus. IDMEF [2], a été conçu pour permettre par exemple à une sonde de détection d'intrusion de communiquer des données précises à un logiciel central de traitement des incidents. Ce dernier peut enregistrer, corréler et/ou présenter les informations issues de la sonde. IDMEF peut également servir de format d'échange entre organisations mais, même s'il est extensible, ses possibilités restent limitées car il a été conçu pour faire que des programmes puissent communiquer entre eux. IODEF, inspiré de IDMEF, a l'objectif plus ambitieux de permettre des échanges entre êtres humains. C'est un format très riche ; la description que l'on peut faire d'un incident peut contenir notamment :

— (une signification) la raison d'exister de cette remontée d'incident (signalement, demande d'investigation, demande de réduction d'impact)

— (des traces) tous les logs , les captures de paquet, les extraits de code binaire , avec les dates d'occurrence

— (des transactions) tout l'historique des actions effectuées

— (des recommandations) l'action attendue de la part du récepteur du fichier IODEF (filtrage d'une adresse IP etc.)

— (des éléments d'inventaire) les machines concernés avec toutes les actions effectuées

— (des contacts) l'ensemble des personnes concernées, de manière structurée (le contact "CSIRT-example" inclus des sous-contacts qui sont les membres du CSIRT)

De plus, ce format est flexible : il fournit des possibilités de mettre des explications en texte libre pour de nombreux éléments. En réalité, très peu d'éléments sont obligatoires. De par sa souplesse, IODEF autorise plusieurs façons de représenter un incident. Il existe de nombreuses extensions et standards associés à IODEF, comme IODEF-SCI, RID. Il existe également des formats spécialisés, comme ARF pour le spam, XCCDF pour valider la conformité à une politique par rapport à des checklists, MMDEF pour décrire des malwares.

2.2 Deux exemples de représentation d'incident

Pour rendre plus concret les informations représentées par IODEF, voici un exemple de représentation d'un scan :

```
<?xml version="1.0" encoding="UTF-8"?>
  <IODEF-Document version="1.00" lang="en"
    xmlns="urn:ietf:params:xml:ns:iodef-1.0"
    xmlns :xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi :schemaLocation="urn:ietf:params:xml:schema:iodef-1.0">
    <Incident purpose="reporting">
      <IncidentID name="csirt.example.com">59334</IncidentID>
      <ReportTime>2006-08-02T05 :54 :02-05 :00</ReportTime>
      <Assessment>
        <Impact type="recon" completion="succeeded" />
      </Assessment>
      <Method>
        <Reference>
          <ReferenceName>nmap</ReferenceName>
          <URL>http ://nmap.toolsite.example.com</URL>
        </Reference>
      </Method>
      <Contact role="creator" type="organization">
        <ContactName>CSIRT for example.com</ContactName>
        <Email>contact@csirt.example.com</Email>
        <Telephone>+1 412 555 12345</Telephone>
      </Contact>
      <EventData>
        <Flow>
          <System category="source">
            <Node>
              <Address category="ipv4-addr">192.0.2.200</Address>
            </Node>
            <Service ip_protocol="6">
              <Portlist>60524,60526,60527,60531</Portlist>
            </Service>
          </System>
          <System category="target">
            <Node>
              <Address category="ipv4-addr">192.0.2.201</Address>
            </Node>
            <Service ip_protocol="6">
```

```
          <Portlist>137-139,445</Portlist>
         </Service>
        </System>
       </Flow>
      </EventData>
     </Incident>
    </IODEF-Document>
```

Les champs utilisés par RENATER pour signaler les incidents sont moins nombreux ; l'exemple suivant indique qu'une machine infectée, appartenant au botnet «Cutwail» a été détectée par RENATER :

```
<?xml version="1.0" encoding="UTF-8"?>
<RENATER-CERT-Document version="1">
 <Incident purpose="handling">
  <IncidentID>20150831-1441009818</IncidentID>
  <SendTime>2015-08-31T10 :30 :18+02 :00</SendTime>
  <Contact role="irt" type="organization">
   <name>CERT-RENATER</name>
   <Email>certsvp@renater.fr</Email>
   <Telephone>+33153942044</Telephone>
  </Contact>
  <Dest>cert@example.org</Dest>
  <Attack>
   <Description>Ver</Description>
   <StartTime>2015-08-31T10 :30 :18+02 :00</StartTime>
   <Source>
    <SourceIP>192.0.2.1</SourceIP>
    <SourceName>compromised-host.example.org</SourceName>
   </Source>
   <Record>
    <RecordLog type="string">2015-08-28 00 :00 :01,00 :00 192.0.2.1 0 2259 FR ALSACE STRAS-
BOURG compromised-host.example.org cutwail 0 0 0</RecordLog>
   </Record>
  </Attack>
 </Incident>
</RENATER-CERT-Document>
```

2.3 La classification des incidents

La typologie des incidents est un aspect délicat de leur formalisation. De la même manière qu'il y a plusieurs façons de les modéliser, il y a plusieurs façons de les classer. Par exemple, un événement de scan peut être considéré comme une tentative d'intrusion, un signe de compromission d'une machine interne, une simple reconnaissance ou du bruit sans intérêt en fonction de la source, de la cible, du contexte, de la politique de sécurité, et de la personne qui classifie l'incident. IODEF est un format relativement pragmatique de ce point de vue et s'adapte à la classification adoptée par l'utilisateur. Malgré les difficultés intrinsèques de la classification, il est recommandé d'en avoir une. Selon notre expérience, classifier les incidents dans des catégories offre de nombreux avantages : cela permet de faire des statistiques, de voir se dessiner des

tendances, etc. Toute classification est initialement incomplète ou ambiguë. Il n'y a pas lieu de s'inquiéter : elle fonctionnera de mieux en mieux au fur et à mesure des corrections qu'on lui apportera (à condition bien sûr de revoir régulièrement sa constitution). Les types d'incidents que nous avons définis sont peu nombreux :

— Compromission de compte utilisateur
— Compromission de poste de travail
— Compromission de serveur
— Atteinte aux droits d'auteur
— Autres

Pour information, à cette liste s'ajoutent deux autres items mais ces incidents ne font pas l'objet d'un traitement automatisé (ils correspondent au vol ou à la perte de matériel ou de données). Dans le cadre de l'outil, la classification n'est pas extraite de la description IODEF mais saisie par l'opérateur. La typologie du CERT Osiris diffère de celle du CERT RENATER : par exemple, là où RENATER signalera un scan issu du réseau Osiris, nous classerons l'incident comme une compromission d'ordinateur (poste de travail ou serveur).

3 ROBOCERT

3.1 Processus de traitement des incidents du CERT Osiris

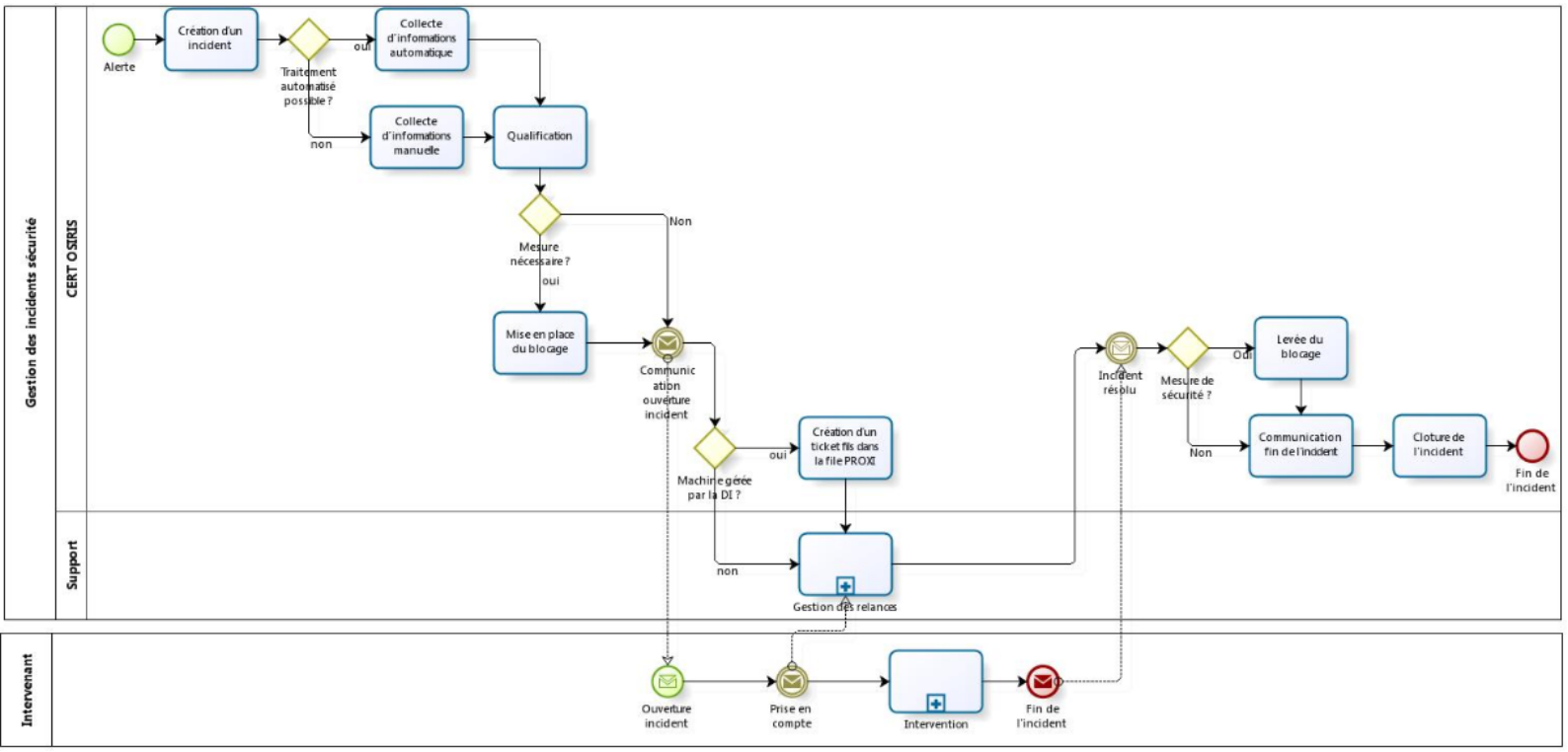

Figure 1 - Processus de traitement des incidents sécurité

Le processus de traitement des incidents a été formalisé depuis 2012. Schématiquement, lorsque l'incident est connu, l'opérateur du CERT procède à son ouverture et à sa qualification. Il collecte les données, fait

une analyse, met en place un blocage éventuel, demande une ou plusieurs interventions à des correspondants. Une fois les interventions et interactions avec les correspondants arrivées à leur terme, il vérifie que l'incident n'a plus d'impact, lève le blocage éventuel et le clôt.

3.2 Fonctionnement de ROBOCERT

Par rapport au processus décrit précédemment, Robocert couvre l'enchaînement des phases initiales du traitement d'incident : ce sont les phases d'ouverture, de collecte, de blocage et de diffusion d'information. Un principe essentiel a été posé dès la conception de Robocert : les personnes sont les acteurs fondamentaux du processus de traitement des incidents. L'outil ne se substitue jamais à leur fonctions en tant qu'acteurs intelligents du système : l'analyse technique de l'incident, le dialogue avec les différents intervenants et toutes les décisions qui ont un impact, comme le blocage d'une adresse, sont faites par des humains. Le flux de données géré par Robocert peut se décrire de la manière suivante : RENATER ajoute dans ses notifications d'incident par mail, en plus du texte en clair, une pièce jointe qui correspond à une représentation structurée de l'incident au format IODEF. Robocert extrait la pièce jointe et l'analyse pour trouver différentes données. Elles sont ensuite utilisées pour interroger automatiquement des référentiels. Les informations trouvées complètent le ticket et servent à analyser l'incident.

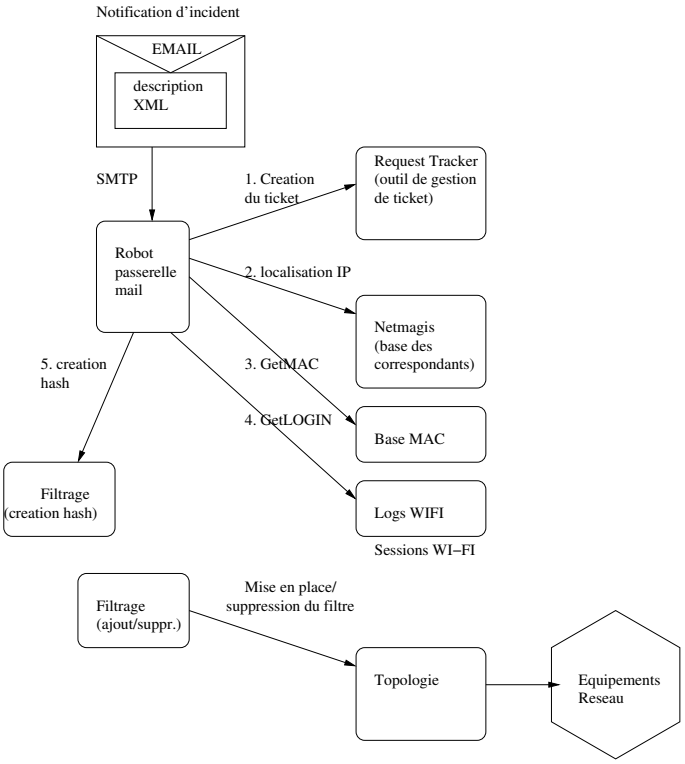

Figure 2 - Schéma des flux de données

3.2.1 Passerelle de messagerie

La passerelle de messagerie est le point d'entrée du système. Le mail contenant la pièce jointe au format IODEF est envoyé à une adresse électronique convenue (par exemple "robocert@example.com"). Cette adresse est un alias qui appelle un programme : Robocert. Robocert lit sur son entrée standard le message et le décompose en différentes parties (en-tête, corps du message, lui-même composé de différents éléments), à

la recherche d'une pièce jointe au format XML. Elle est analysée et plusieurs informations en sont extraites : l'adresse IP source de l'attaque, les heures de début et fin d'incident et l'identifiant de l'incident d'origine utilisé comme référence dans les communications avec le CERT RENATER.

3.2.2 Système de ticket

Robocert crée ensuite un ticket d'incident dans le système de gestion de ticket, Request Tracker [3], dans une file spécifique, celle des incidents du CERT. Ce ticket aura un numéro distinct de l'identifiant RENATER. Ce numéro sera utilisé pendant toute la durée de l'incident. Le ticket va ensuite être complété par des données issues de référentiels et d'applications permettant de faire des recherches dans des fichiers de journalisation. L'infrastructure du système de ticket apporte un cadre structurant au traitement :

— l'attribution d'un identifiant unique d'incident,

— la possibilité de lier/fusionner d'autres incidents,

— la notification systématique des acteurs par courrier électronique,

— la gestion fine des droits d'accès aux informations,

— la visibilité immédiate du statut des incidents,

— la richesse et l'extensibilité des métadonnées, comme le champ "type d'incident", qui propose une sélection de valeurs parmi les éléments de typologie qui ont été définis,

— la possibilité de faire des recherches avancées et des statistiques,

— une traçabilité détaillée des actions effectuées (réponses, actions de filtrage, etc.).

3.2.3 Collecte d'informations

Une fois les données extraites de l'attachement IODEF, Robocert va les utiliser pour collecter différentes informations. Cette collecte va accéder à un ensemble de web-services qui s'appuient sur des référentiels : les sous-réseau IP, la base des correspondants réseau, etc. La source de ces informations est l'application Netmagis qui les stocke dans une base de données. La première requête va interroger le référentiel des sous-réseaux en transmettant l'adresse IP. Le web-service renverra le préfixe du sous-réseau incluant l'adresse et une description du réseau.

Exemple :

```
[Request]
        GET /net/?ip=198.51.100.17
[Answer]
        {
            "network": "198.51.100.0/24",
            "description": "subnet de test labo Alpha"
        }
```

La deuxième requête permet de déterminer les identifiants des correspondants responsables de ce sous-réseau, classé par groupe de correspondant, et leurs coordonnées :

```
[Request]
       GET /resp/?net=198. 51. 100. 0/24
[Answer]
        {"groups": [
```

```
                "laboratoire A": ["jules","marcel","anthony"],
                 "composante X": ["dave","fred"],
                ],
         "contact":  [
                "jules":{"mail":"jules@example.com",
                                "cn":"Jules Schmidt"
                        },
                "fred": {"mail":"fred@example.net",
                                "cn":"Fred Dupond"
                        },
                . . .
                ]
        }
```

Les informations les plus importantes ont été collectées, à savoir la localisation de l'adresse et les correspondants locaux responsables. Toutes les étapes suivantes de la collecte sont optionnelles :

— la détermination de l'adresse MAC pour pouvoir localiser la machine sur un équipement réseau précis,

— pour certaines adresses IP, l'identification d'un utilisateur par son adresse et les heures de début et de fin (via la recherche les journaux de connexion des services wifi et VPN).

Toutes les informations collectées sont intégrées dans le ticket. Les coordonnées des responsables sont notamment ajoutées par Robocert dans les méta-données du ticket en tant que personnes à notifier, ce qui permet de leur communiquer automatiquement chaque action effectuée.

3.2.4 Blocage d'adresse

Une fois la collecte effectuée, Robocert crée également une commande de blocage de l'adresse IP concernée, commande qui peut être actionnée ou non par l'opérateur. Cette commande est créé via un web-service, en indiquant l'adresse et le numéro du ticket. Le web-service crée simplement une clef tirée aléatoirement et enregistre en interne l'adresse IP associée à cette clef. La clef est opaque, puisque l'adresse IP n'est pas visible de l'extérieur, et au vue de sa longueur, elle résiste bien à une attaque de "force brute" consistant à énumérer toutes les valeurs possibles. La clef est envoyée en retour suite à la requête de création :

```
[Request]
  /create/<Id>/<Adresse IP>
[Answer]
  5b6edd79c9551e1a279b6f9dc7c53e34
```

L'exécution de la commande de blocage, une fois que l'opérateur a décidé de bloquer l'adresse se fait par un autre web-service, en indiquant simplement la clef :

```
  /filter/<Hash>
```

Le blocage est alors mis en place par un outil de configuration d'équipement réseau (Rancid) sur les routeurs. Pour lever le blocage, on procède de manière similaire :

```
  /unfilter/<Hash>
```

Robocert crée lui-même la commande de filtre, récupère la clef, et ajoute dans le ticket des liens directement cliquables par l'opérateur pour filtrer et défiltrer l'adresse. Exemple des commandes incluses dans le ticket :

```
Pour filtrer l'adresse 198.51.100.51 :
  https://myblock.example.com/filter/fe285413c5f8e37c8cbb9412c4e1fee2

Pour defiltrer l'adresse 198.51.100.51 :
  https://myblock.example.com/unfilter/fe285413c5f8e37c8cbb9412c4e1fee2
```

Une fois le blocage levé, la clef est effacée. Étant donné la sensibilité de l'opération, la sécurité de ce web-service a été renforcée : le web-service est filtré au niveau réseau et seuls les postes d'un réseau bien identifié peuvent y accéder. De plus, une authentification de l'utilisateur est exigée. Il existe par ailleurs une autre application qui permet de visualiser les adresses actuellement filtrées et de lever le blocage sur la base de l'adresse IP.

3.3 Forces et faiblesses

3.3.1 Organisation et référentiels

Le contexte pèse un poids non négligeable dans le fonctionnement de l'outil. En général, les équipes du CERT et celles qui opèrent le réseau et qui sont donc capables de mettre en place des blocages d'adresse IP sont bien distinctes. Ce n'est pas le cas ici : le CERT Osiris comporte parmi ses membres plusieurs personnes de la Direction Informatique, qui assurent des fonctions de sécurité et des fonctions dans d'autres domaines, et notamment dans le domaine du réseau. De plus, il y a une collaboration étroite entre le CERT et tous les collègues de la Direction Informatique pour les interventions liées à des incidents. Le fait que les équipes s'occupant de sécurité et de réseau soient proches fluidifie le traitement des incidents et rend plus aisée la mise au point d'un outil comme Robocert. Mais, même dans des organisations où les deux équipes seraient moins liées, la création d'API simples et sécurisées implémentant des recherches dans des référentiels et des blocage réseau est un gain pour tout le monde. De même, l'automatisation dépend fortement de la maintenance des référentiels. Elle oblige à corriger rapidement les erreurs et à faire évoluer les référentiels, et c'est un avantage plutôt positif pour la qualité de ces outils communs que constituent les référentiels.

3.3.2 Le problème du NAT

Le principale problème dans le traitement des incident est lié à la translation d'adresse, (NAT, pour Network Address Translation). À ce problème s'ajoutent également des contraintes de nature organisationnelle. Comme évoqué ci-dessus, dans notre contexte, les personnes qui gèrent la sécurité et le réseau proviennent sensiblement du même périmètre :

— les applications de l'université, hébergées sur les serveurs de la Direction Informatique,

— le réseau jusqu'à la prise et le poste de travail pour certains utilisateurs dans les composantes contractualisées.

Le CERT Osiris peut cependant bloquer une adresse IP, car au niveau politique, il lui a été accordé un pouvoir d'intervention et de blocage en cas d'incident. Mais il y a des structures qui sont simplement raccordées au réseau, et pour lesquelles la Direction Informatique joue le rôle d'opérateur réseau. La DI n'a pas de visibilité au delà de la limite de responsabilité constituée par l'équipement réseau en entrée d'un bâtiment. Elle ne peut donc pas intervenir sur le réseau interne. Si ces structures utilisent du NAT, la source

de l'incident est indéterminable : une IP publique correspond à des dizaines voire centaines d'adresses IP privées. De plus, la recherche de l'adresse interne requiert l'accès aux journaux des sessions NAT. Cette recherche exige de fournir d'avantage d'informations : les adresses et ports sources et destination, et les heures précises de communication. Plusieurs approches sont possibles pour affiner la réponse à l'incident et présenter l'adresse interne directement exploitable :

— décliner un système de gestion d'incident similaire dans chaque structure, alimenté via le mail par robocert,

— disposer d'un accès aux logs, restreint au CERT et autorisant uniquement la recherche de journaux de connexion.

— exporter les journaux de connexion vers le CERT, avec un engagement signé sur la confidentialité des données. Une fois l'adresse interne déterminée, le blocage de l'adresse reste sous la responsabilité de la structure.

Dans tous les cas, la redéfinition de la limite de responsabilité, le surcroît de complexité et l'investissement en temps et en argent pour développer ces solutions sont des obstacles importants pour lever cette difficulté.

4 Évolutions/perspectives

Une piste d'évolution de Robocert pourrait être la reconnaissance de formats supplémentaires. Par exemple :

— IDMEF pour les messages issus des sondes de détection d'intrusion,

— ARF [4] (Abuse Report Format) pour le spam,

— ACNS [5] pour le piratage de fichier sous copyright,

— des modèles d'incident qui nous serait spécifiques mais dont le format s'appuierait sur IODEF.

Dans ce dernier cas, l'idée serait d'injecter dans Robocert, sans doute de façon semi-automatisée, des mails avec ces nouveaux formats. Ces mails proviendraient de différentes sources. Exemples :

— une sonde qui détecterait des envois d'un nombre trop élevé de mail pour un utilisateur donné (fréquemment signe d'une compromission de compte suite à un phishing réussi)

— un IDS tourné vers le réseau interne qui détecterait des motifs de compromission de machines définis.

5 Conclusion

L'automatisation du traitement des incidents, en évitant les tâches fastidieuses et en limitant les erreurs de saisie, fait gagner du temps et augmente la qualité du processus. Mais elle ne pourra qu'augmenter le niveau de sécurité très indirectement. En définitive, le traitement des incidents est très lié aux interactions entre le CERT et ses correspondants sur le terrain qui interviennent sur les éléments compromis (serveurs, postes de travail, comptes utilisateurs etc.). Le niveau de formation, la disponibilité et la réactivité des correspondants sont des aspects déterminants pour la qualité globale de la réponse aux incidents. Il y a bien d'autres facteurs qui améliorent cette qualité, et notamment la baisse du nombre d'incidents. C'est évidemment une approche globale qu'il faut avoir. Quels que soient les efforts investis dans l'automatisation du traitement, une démarche pro-active en matière de sécurité, résultant d'une concertation entre le CERT et les parties prenantes est essentielle pour faire baisser le nombre des incidents. Les autres activités du CERT en matière d'analyse de risque et de conseils en architecture de sécurité complètent avantageusement l'automatisation du traitement des incidents.

Bibliographie

[1] R. Danyliw, J. Meijer, et Y. Demchenko. The incident object description exchange format, décembre 2007. https://www.ietf.org/rfc/rfc5070.txt.

[2] H. Debar, D. Curry, et B. Feinstein. The intrusion detection message exchange format (idmef), mars 2007. https://www.ietf.org/rfc/rfc4765.txt.

[3] Jesse Vincent, Robert Spier, Dave Rolsky, Darren Chamberlain, et Richard Foley. *RT Essentials*. O'Reilly Media, 2005.

[4] Y. Shafranovich, J. Levine, et M. Kucherawy. An extensible format for email feedback reports, août 2010. https://www.ietf.org/rfc/rfc5965.txt.

[5] Automated copyright notice system (acns) 2.0, 2015. http://www.acns.net/v1.3/ACNS%202_0_v1.3.pdf.