provadys

SOC

SOC PROVADYS

Bilan de 2 ans au service des PME / ETI françaises

Auteur :

Julien Steunou, Lead SOC Provadys

Fin 2016, Provadys lançait son **SOC dédié aux PME / ETI (entreprise de taille intermédiaire) françaises** avec pour objectif de mettre à leur disposition des services spécifiques de protection, détection et réponse aux incidents de sécurité adaptés aux menaces qui les concernent et à leurs moyens.

Convaincu que ce marché ne pouvait pas être adressé efficacement par des solutions SOC «grand compte» simplement remises à l'échelle, le choix de Provadys a été de repartir de la base pour concevoir des services intégrant de manière native les spécificités propres au contexte des PME / ETI. La vision de Provadys repose sur la conviction que même si toutes les entreprises ont besoin de SSI, la façon d'atteindre la Sécurité n'est pas la même pour toutes.

Que vous soyez en réflexion, en cours de construction d'un SOC ou que vous souhaitiez comparer votre SOC actuel à notre vision du SOC spécifique aux PME / ETI, vous trouverez ci-dessous les principaux enseignements tirés de deux années pleines d'opérations de détection et de gestion des vulnérabilités pour 12 PME et ETI et plus de 25 missions significatives de réponse à incident. Ce qui ressemblait à un pari il y a deux ans est aujourd'hui pleinement réussi et maintenant confirmé par l'expérience du SOC NetXP avec lequel Provadys a initié le rapprochement fin 2018.

1 L'importance de bien aligner, en toute transparence, le SOC sur des menaces & adversaires pertinents

Toutes les PME / ETI n'ont pas la possibilité de structurer un programme cyber défense. Pour de nombreuses organisations, le point de départ d'un projet SOC est souvent un besoin assez urgent, en réaction à un incident de sécurité, une exigence business venant d'un client ou la prise en compte d'une nouvelle exigence réglementaire.

Le besoin d'un SOC est très souvent exprimé sans un cadrage des menaces considérées et avec beaucoup d'incertitudes sur le périmètre et les volumes de données à traiter.

Accompagner une PME / ETI demande alors de la méthode pour définir les événements redoutés qui sont pertinents de prendre en compte, poser une stratégie de défense avec une trajectoire d'amélioration et gérer les dépendances techniques.

Il est essentiel de ne pas faire de la sur-qualité mais également de ne pas tromper, même par omission, le client sur la réalité de la capacité dont il se dote. Deux écueils à éviter sont de :

> Présumer que le besoin est de lutter contre toutes les organisations et dimensionner un dispositif en conséquence, avec un budget complètement irréaliste pour une PME / ETI qui peut décourager une organisation de mettre en place une solution adaptée.
> Dimensionner un dispositif à minima, et laisser les responsables penser à tort que le SOC qu'ils achètent est efficient contre tout type de menaces

Pour la plupart des PME / ETI, l'objectif réaliste est de contrer la cyber criminalité et certaines menaces internes, pas de lutter contre des groupes soutenus par des états !

Pour un expert sécurité, accompagner une PME / ETI demande de caler son référentiel de

menaces sur ces enjeux et d'accepter de mettre de côté des attaques / adversaires pointus, sujets sexy mais souvent peu pertinent pour son client. En se dédiant dans la durée aux PME / ETI tout en restant en prise avec ce qui se fait dans les grands comptes et les secteurs exposés à des menaces pointues, nous avons constaté que l'équipe rend des services plus pertinents pour ses clients tout en trouvant une grande satisfaction dans ce qu'elle délivre.

L'équipe SOC Provadys a progressivement amélioré une méthodologie, essentiellement basée sur la modélisation par killchain, l'utilisation de référentiels comme MITRE ATT&CK et le retour des équipes sécurité offensive Provadys pour identifier des événements redoutés en termes de scénarios plausibles d'attaques & adversaires et construire un chemin de prise en compte progressive, listant les dépendances sur les données / moyens de collecte de log et les mesures de sécurité à déployer pour atteindre les objectifs.

Cette méthodologie est au cœur des missions de cadrage que nous réalisons mais également des projets de prise en charge et de l'amélioration continue des services.

Cette approche permettant de savoir contre quels adversaires l'entreprise souhaite se protéger et quelles sont les méthodes d'attaque qui sont susceptibles d'être déployées place régulièrement le SOC Provadys au centre de la stratégie sécurité des PME / ETI clientes. Cela permet de challenger toutes les mesures de sécurité existantes et les futurs investissements par rapport à leur contribution mesurée ou attendue en détection, blocage, perturbation voire désinformation d'un adversaire dans une étape d'un scénario d'attaque.

La démarche peut paraitre complexe au premier abord mais il n'en est rien : c'est abordable pour tout type d'organisation, avec à la clé des résultats, un exercice intéressant et stimulant, et la satisfaction de maîtriser sa sécurité et de prendre des décisions éclairées, loin de la pression d'un supposé état de l'art de la sécurité ou du marketing de tel ou tel vendeur.

2 La nécessité de s'adapter à la capacité de traitement des incidents de sécurité de l'entreprise

La ressource la plus rare et précieuse de nos clients PME / ETI est le temps de leurs équipes.

Construire un SOC pour les PME / ETI suppose un travail de qualification des incidents important et engagé, avec une sensibilité différente d'un SOC pour les grands comptes. Dans ces derniers, la notification est quasi systématique dès qu'il y a un doute (tendance souvent traduite dans les engagements contractuels, indicateurs et pénalités) et elle induit une surcharge / fatigue des équipes internes ou finalement une tendance à ignorer les informations remontées par le SOC.

La bonne sensibilité pour une PME / ETI suppose que le SOC ait une large autonomie de vérification et ne notifie activement les équipes clients que sur les incidents avérés ou lorsqu'une levée de doute rapide est importante.

Cela implique une responsabilité importante et le fait que parfois le SOC va se tromper et rétrospectivement se rendre compte qu'il aurait dû notifier une alerte se transformant en incident de sécurité avéré.

Porter cette responsabilité pour un prestataire SOC suppose une réelle confiance de son client, un cadre contractuel adapté et une démarche d'amélioration continue de leur performance commune. Si la confiance réciproque n'est pas établie ou le contrat trop punitif, la logique de notification au plus tôt systématique va se mettre en place au détriment de l'efficacité du traitement réel.

Nous avons observé qu'une équipe SOC a le plus grand mal à opérer des contrats avec des sensibilités radicalement différentes, les analystes ne pouvant pas changer de logique de qualification en permanence. Cela nous a convaincu qu'établir une équipe dédiée PME /

ETI avec un état d'esprit constant permet d'opérer un service adapté.

Enfin il est essentiel pour la réussite des services que le SOC soit impliqué plus fortement dans l'accompagnement des équipes clients d'une PME / ETI que dans celles d'un grand compte pouvant déjà disposer d'un CSIRT / CERT interne dans l'organisation de la réponse aux incidents de sécurité et dans leur suivi opérationnel et le détail des recommandations de traitement.

Le suivi des incidents de sécurité allant plus loin, cela déplace également le point de bascule dans un mode d'expertise de réponse à incident. Savoir quand sortir du mode SOC forfaitaire pour proposer un dispositif de réponse avec des experts intervenants à distance ou projeté sur site, et donc généralement facturés au temps passé, demande également une sensibilité et une confiance mutuelle.

3 L'apport des moyens de vigilance externe

Souvent méconnu des PME / ETI, les moyens de vigilances externes peuvent ne pas faire partie des besoins exprimés dans un projet SOC.

Pour autant, si le renseignement sur les menaces (threat intelligence) est au cœur des stratégies de détection des SOC modernes, il ne faut pas oublier que les adversaires se renseignent également et choisissent leurs victimes en fonction du renseignement disponibles et de la surface d'attaque exploitable qu'ils constatent.

Aussi il est souvent très intéressant pour une entreprise de déployer des moyens de détection permettant d'être alertée de :

> L'évolution défavorable de la surface d'attaque externe, par exemple l'exposition d'un service de contrôle à distance sur un serveur web lors d'une opération de mise à jour, ouvert à tout Internet par confort et non refermé en fin d'opération)
> L'usurpation de votre identité, que ce soit par l'enregistrement d'un domaine pouvant passer pour le vôtre pour monter un site malveillant ou l'utilisation de votre domaine pour envoyer des campagnes de mails malveillant
> La disponibilité de documents sensibles sur le NAS personnel d'un employé / sous-traitant / partenaire mal configuré et laissant en accès libre des sauvegardes professionnelles mêlées à des données personnelles.
> L'exposition sur des sites type pastebin de couples d'identifiants / hash de mots de passe valides issus d'une base client d'un site e-commerce tiers qui s'est fait compromettre et dont sont clients plusieurs de vos employés (qui auront utilisé leur adresse mail professionnelle et le même mot de passe qu'en interne à la création de leurs comptes !)

Tous ces événements peuvent être détectés par des moyens de vigilance externe qui apportent souvent beaucoup de valeur pour un investissement modeste et surtout peu engageant : n'étant pas en adhérence avec votre système d'information, ils peuvent être testés, déployés (et résiliés) très facilement.

Le SOC Provadys a engagé dès sa création des moyens importants pour innover sur ces modules de détection et en a dérivé une solution d'évaluation de la maturité sécurité (Security Rating).

En effet les informations publiques exploitées par vos adversaires alimentent également les moteurs de notation de la maturité sécurité de plus en plus utilisés par vos assureurs, banquiers, investisseurs et clients ayant à cœur d'évaluer la sécurité de leurs fournisseurs.

Travailler sur cet axe de vigilance externe est bénéfique sur le plan de la sécurité mais également sur la perception générale de votre niveau de sécurité, et donc de la confiance que peuvent avoir des tiers.

4 Le challenge de la gestion des vulnérabilités

La gestion des vulnérabilités est un sujet sur lequel les PME / ETI ne peuvent faire l'impasse. Faire reposer son système d'information sur des infogérants ou des services cloud permet d'évacuer une partie de la gestion technique des vulnérabilités mais il reste toujours des vulnérabilités à traiter et un problème de taille : les équipes n'ont pratiquement jamais le temps de remédier à toutes les vulnérabilités / tout patcher.

Dans ce contexte, un SOC au service des PME / ETI doit savoir apporter la bonne information et aider à la décision pour prioriser les actions et faire en sorte que si l'équipe IT a le temps de patcher dix actifs dans le trimestre, son énergie passe dans la remédiation des 10 vulnérabilités qui présentent le plus de risque d'exploitation / impact.

Mettre à disposition dans un portail une masse d'informations sur les vulnérabilités n'est pas la bonne réponse : l'information sur les vulnérabilités doit être sélectionnée par le SOC et apportée au bon moment aux bonnes personnes et alimenter un processus de décision que le SOC aide souvent à mettre en place et structurer.

C'est à ces conditions, et en responsabilisant les responsables d'applications et de domaine technique, que des PME / ETI sont parvenues à mettre en place un processus de gestion des vulnérabilités qui fonctionne, avec une amélioration progressive et mesurée du temps d'exposition aux vulnérabilités avant remédiation.

5 Le besoin de sécurité budgétaire

Au-delà du dimensionnement du budget, la plupart des PME / ETI ont une exigence légitime de pouvoir prévoir l'évolution du budget sur plusieurs années et d'avoir une maitrise de dernier.

Le coût du service SOC externe, finançant le projet de prise en charge initial, des moyens techniques de détection et une certaine « bande passante » d'analyste SOC, peut être source d'incertitude.

Nous rencontrons souvent dans les expressions de besoin un périmètre constitué d'une description technique du système d'information, avec peu ou pas de métriques sur les volumes de données à considérer (et pour cause, la plupart des clients n'ont pas au départ réalisé de projet de gestion des logs assurant la collecte et centralisation de ces derniers, ne serait-ce qu'avec un serveur syslog).

Constituer des hypothèses sur les volumes de log est un exercice extrêmement périlleux. Comme tous les SOC, nous disposons d'abaques en fonction des types de sources / nombre d'utilisateurs mais notre expérience montre que les écarts type sont énormes d'une PME / ETI à l'autre et peuvent complétement modifier un budget.

Pour apporter de la sécurité budgétaire, le point de départ de la réflexion ne doit pas être focalisé sur la définition technique d'un périmètre / partie du système d'information.

La bonne approche est de partir du cadrage en terme d'événements redoutés et de travailler pour chercher en permanence la meilleure détection dans une enveloppe de moyens humain et technique donné.

Cela suppose :

> Un dimensionnement d'équipe d'analystes SOC cohérents pour traiter les alertes des scénarios de détection et animer une « usecase factory » produisant de nouveaux scénarios de détection au fur et à mesure que ceux en production deviennent matures et ne produisent plus de faux positif
> Évaluer et adresser progressivement les dépendances techniques en termes de données pour alimenter les scénarios de détection et parfois décider d'écarter des scénarios trop coûteux à opérer.
> Identifier des paliers de dimensionnement des moyens techniques en termes de volume de données / log puis arbitrer dynamiquement l'intégration de sources de logs dans les moyens techniques en fonction de leur apport, et ne pas hésiter à collecter certains logs dans des solutions moins coûteuse d'où ils pourront être tiré dans le cadre d'une investigation.
> L'utilisation de solutions techniques où les volumes de données ont un impact financier minimum (ce qui implique de ne pas utiliser la solution la plus déployée sur le marché, qui, bien qu'excellente techniquement, est basée sur une notion d'événements par seconde introduisant encore plus de volatilité économique).

Il est enfin essentiel pour une PME / ETI d'anticiper la charge de travail et le budget associé sur le traitement des incidents de sécurité. Même avec un SOC adapté notifiant des incidents pertinents et assurant un bon suivi, les incidents standards doivent être traités par les équipes internes.

Ce point est un facteur d'échec de projets SOC que nous rencontrons encore régulièrement dans les organisations qui n'ont pas anticipé cette charge ou pensé / été amené à croire que cette tâche pouvait s'externaliser complétement.

Traiter des incidents de sécurité demande de l'intimité avec le système d'information, la production IT, les métiers, du temps pour orchestrer le traitement avec de nombreuses parties prenantes d'une organisation (RH, juridique…) et du temps sur les équipes IT pour réaliser les gestes techniques.

Pour fonctionner, un SOC câblé pour opérer pour de large organisation va soit considérer qu'il y a une équipe typée CSIRT / CERT interne qui va s'organiser, soit proposer un mode hybride avec des experts détachés sur site client ou de prendre en infogérance complète le système d'information.

Ces approches sont possibles mais doivent être présentées dès le départ, et non comme c'est très souvent le cas apparaître dans un second temps, une fois que les difficultés apparaissent. Reste également que si elles fonctionnent pour des incidents de sécurité techniques, les limites apparaissent vite sur des incidents de sécurité liés à des problèmes de fuite de données ou impliquant des employés.

L'expérience du SOC Provadys montre également que des organisations, bien accompagnées, peuvent mettre en place une capacité de réponse efficace (pouvant évoluer en CSIRT), en capitalisant sur des ressources IT et/ou sécurité assurant ce rôle en roulement.

Associé à la contractualisation d'un service de réponse à incident (éventuellement par le biais d'une cyber assurance) pour pouvoir déclencher une aide externe sur les incidents complexes avec des engagements de délais d'intervention, cette organisation permet de faire face à toutes les situations.

6 L'évolution de la réponse automatisée

Pendant longtemps la position des SOC cyber défense a été de se tenir à l'écart de la gestion des changements sur les équipements de sécurité, activité qui, si elle a au départ été dans les attributions d'un SOC, a migré depuis plusieurs années dans le périmètre des NOC.

Cette position avait du sens car réaliser des gestes techniques sur des équipements de production nécessite une prise de responsabilité opérationnelle, de l'expertise technique produit souvent peu représentée dans les équipes d'analystes et aussi un mélange de responsabilité permettant à une activité de faire disparaitre les erreurs de l'autre.

Le développement des API dans tout l'écosystème technique et le développement d'outil de réponse à incidents permettant de coder des playbook de réponse ont ouvert la voie à un nouveau changement avec l'industrialisation et l'automatisation de certaines réponses techniques. Via les API, certains changements de configuration deviennent possibles dans un cadre maitrisé (les changements de configuration pour lesquels une procédure est définie), sans nécessité de connaissance produit par l'analyste SOC qui déclenche l'opération et avec une grande traçabilité de ce qui est réalisé.

Un SOC externe est alors à même d'aller en toute autonomie bloquer un flux sur un firewall impliquant des IP malveillantes ou mettre en quarantaine les mails provenant de certains domaines. Il est également possible de prévoir des actions plus complexes comme la suppression de mails identifiés comme malveillants dans la messagerie des utilisateurs ou l'isolement de poste de travail compromis.

L'automatisation de la réponse permet alors une meilleure réactivité dans le traitement de certains incidents et un gain de temps considérable pour les équipes IT de l'organisation. L'effort d'intégration est réel mais abordable et vite rentabilisé sur des incidents avec une haute occurrence.

7 La nécessité de souscrire à une assurance cyber

L'offre d'assurance cyber s'est considérablement développée ces dernières années, y compris pour les PME / ETI avec des polices adaptées à chaque situation et permettant de gérer les conséquences financières d'attaques cyber.

Ces produits sont désormais accessibles et matures. Les bons contrats ont des couvertures des sinistres et des clauses d'exclusion des garanties cohérentes.

En revanche il est important de savoir que beaucoup d'assureurs évaluent la maturité sécurité cyber de leurs clients / prospects via des systèmes de notation travaillant sur les données publiques et le niveau de sécurité qu'il est facile de constater & tester de façon automatisée depuis Internet. Souscrire des services SOC de vigilance externe (tel que décrit précédemment), permet généralement d'améliorer sa notation et de bénéficier de solutions d'assurance plus intéressantes.

Les assureurs peuvent également mobiliser des réseaux d'experts, que ce soit sur les aspects techniques de la réponse à incident, mais également sur des aspects juridiques ou communication.

Conclusion

La cyber défense efficace des PME / ETI ne passe ni par le déploiement de solutions techniques standards sur étagère, ni par la remise à l'échelle de solutions pensées pour des grandes entreprises.

L'efficacité se trouve dans une approche sur mesure mettant au centre :

> Une relation de confiance et de proximité entre un prestataire SOC et un client.
> Une définition claire des adversaires et événements redoutés à gérer.
> Une prise en compte de la réalité des méthodes d'attaque.
> Un programme équilibré entre les capacités d'anticipation des menaces, de protection, de détection, de réponse aux incidents et de retour à la normale.
> La prise en compte de la capacité à faire des équipes internes, et l'anticipation de la charge de travail induite sur les équipes sécurité et IT pour ce que personne ne peut faire à leur place : traiter les incidents de sécurité standards avec leurs connaissances des systèmes, des métiers, des personnes.
> La mise en œuvre de moyens de réponse automatisée dans des scénarios maitrisés, où le SOC va déclencher des changements de configurations via API sur certains équipements de sécurité et faire gagner l'entreprise en réactivité sans charger les équipes IT.
> Une dynamique apportant des résultats rapidement et laissant une grande place à l'amélioration continue.
> Un cadrage budgétaire permettant d'être prédictible financièrement, associé à un pilotage agile de la capacité de détection pour trouver le meilleur équilibre entre les moyens et les événements redoutés couverts.
> L'acceptation qu'en dépit de tous les efforts déployés, il y aura des incidents de sécurité, mais que ces derniers seront gérés efficacement pour en limiter les impacts et que les données nécessaires à la compréhension de ce qui s'est passé seront disponibles.

> Une mécanique d'assurance pour gérer les conséquences financières des attaques cyber.

Beaucoup d'éléments méthodologiques ci-dessus (et de moyens techniques pour les mettre en œuvre) sont partagés entre un SOC PME / ETI et un SOC grand compte.

En revanche l'état d'esprit vis-à-vis des menaces, le niveau d'engagement dans la qualification des alertes et l'acceptation du risque d'erreur d'appréciation des analystes SOC doivent être fondamentalement différents pour être efficace dans l'un ou l'autre des modes.

Passer de l'un à l'autre est évidemment possible, voir souhaitable dans le parcours professionnel d'un analyste, mais opérer deux modèles de service en simultanés pour des clients différents se fait forcément au détriment des PME / ETI : le confort de notifier sans prendre de risque et l'attirance naturelle des experts sécurité pour les scénarios d'attaque pointus a vite raison de toute bonne volonté de bien faire !

Aussi la raison d'être d'un SOC dédié aux PME / ETI va bien au-delà d'un positionnement marché pour le prestataire ou de la recherche d'un meilleur prix / d'une relation plus équilibrée pour un client : c'est la garantie d'un service efficace pour l'entreprise et d'une démarche intéressante pour toutes les parties prenantes !