

LE SIEM AMÉLIORE L'ENSEMBLE DES ACTIVITÉS DES ENTREPRISES ET AIDE LES DIRIGEANTS À RELEVER LEURS DÉFIS CONCERNANT LA CYBERSÉCURITÉ



ÉDITION JANVIER 2020

Les services **SIEM** deviennent incontournables et apportent **4 bénéfices aux entreprises** :

- 1) Soutien légal, traçabilité des informations, preuves
- 2) Support à la conformité des normes : prouver sa bonne foi aux autorités d'audits
- 3) Assistance aux ressources humaines
- 4) Outil de contrôle financier

Qu'est-ce qu'un SIEM?

Au-delà d'amener un meilleur contrôle en regard à la cybersécurité, **le SIEM a une portée beaucoup plus grande en entreprise dans l'ensemble de ses opérations** : soutien légal par la traçabilité des informations et la transmission de preuves, gain de temps par des rapports de conformité automatisés prouvant votre bonne foi lors d'audits, outils d'appui aux ressources humaines en situations de litiges... **Le SIEM permet de limiter les dommages financiers et le déficit d'image de marque. D'éviter que l'image de marque soit ternie.**

Depuis le dernier évènement de cybersécurité survenu chez le Mouvement Desjardins, les dirigeants sont maintenant concernés face aux faits des risques d'attaques qui deviennent de plus en plus importantes et de plus en plus dommageables.

À l'ère où les entreprises de toutes tailles font face aux mêmes enjeux et défis, s'adapter est un passage obligé. Un grand nombre adoptent les **nouvelles technologies comme le nuage et la mobilité** sans compter qu'on encourage l'accélération de la **transformation numérique** au Québec. Il en résulte **un environnement informatique hybride, divers et complexe**, jamais vu auparavant et où se côtoient plusieurs technologies. **D'où l'importance grandissante d'avoir des outils adaptés à cette nouvelle réalité.**

Basés sur l'intelligence artificielle, les solutions SIEM d'aujourd'hui permettent à votre entreprise de réagir rapidement et avec précision en cas de menace ou de fuite de données. Elles donnent en temps réel l'information pertinente et essentielle.

Le SIEM (Security Information and Event Management OU Gestion de l'information et des évènements de sécurité) sert à détecter les anomalies de comportement et les attaques. Il permet de détecter, de diagnostiquer et de prendre action beaucoup plus rapidement.

Nous avons regroupé en 4 catégories les bénéfices qu'apporte le SIEM aux entreprises afin de mieux répartir l'information qui est substantielle. Vous noterez que certains éléments peuvent se retrouver dans plus d'une catégorie.

1) Soutien légal, traçabilité des informations, preuves

Avec le SIEM, vous avez en place des outils automatisés vous permettant de fournir sur demande les documents lorsque demandés par les autorités légales, réglementaires, ou commerciales – bureaux d'avocats, compagnies d'assurances, banques – ou requis lors d'audits:

- Capture de fichiers en vue d'analyse pour preuves légales;
- Historique des permissions de vos usagers en termes d'accès réseau;
- Qui a donné des accès non autorisés à un employé;
- Qui était et qui est toujours administrateur de vos systèmes;
- L'utilisation subversive de comptes de services et autres stratagème afin d'opérer incognito sur le réseau
- Détection d'activités suspectes grâce à la corrélation de plusieurs métriques.

À partir d'une console centralisant les informations, le SIEM apporte une vue globale sur l'ensemble du réseau autant pour les activités que les permissions : qui fait quoi et quand sur les serveurs, qui accède à quoi sur le réseau et particulièrement sur les serveurs, qui a modifié les configurations, **les permissions des usagers tel que l'accès aux répertoires de l'entreprise**, etc.

Le SIEM amène également une assurance de traçabilité vous permettant d'extraire des rapports: journaux d'évènements en cas de litige, appui aux suivis des audits, etc. **Il vous permet de prendre des décisions fondées sur des preuves.**

2) Support à la conformité des normes

Le SIEM permet de satisfaire aux exigences légales de conformité de votre entreprise. Il collecte des données et les place dans un référentiel central à des fins d'analyse de tendances. La génération de rapports de conformité est ainsi automatisée et centralisée. Les opérateurs comme les dirigeants ont accès à des vues d'indicateurs personnalisés et peuvent **alléger la charge des audits en générant eux-mêmes des rapports.**

Le SIEM répond donc à plusieurs exigences de sécurité (historisation, rapports de sécurité) pouvant **générer sans effort des rapports hautement personnalisables** selon les exigences des différentes réglementations.

3) Assistance aux ressources humaines

Le SIEM constitue **un outil de gestion puissant qui apporte aux ressources humaines de l'information essentielle** en situations de litiges ou de résolutions de crises. Il réduit la pression et favorise ainsi **la rétention des employés**.

Grâce à l'intelligence artificielle amenant une capacité d'apprentissage constant, le SIEM en vient à connaître les **comportements habituels de vos usagers et détecte les changements d'habitudes et activités suspectes**. Ceci devient encore plus intéressant dans un contexte où le travail à distance est de plus en plus fréquent.

Lors de vos rencontres de ressources humaines, vous avez donc des écrits appuyant votre démarche – avis et congédiement – et vous permettant :

- L'assainissement de la gestion de vos ressources matérielles et humaines;
 - Mauvaise utilisation du matériel informatique de votre organisation : mobiles, utilisation d'internet à des fins personnelles (recherche d'emploi, Facebook, SMS), installation de logiciels non autorisés mettant à risque l'entreprise;
 - Vous savez ainsi comment vos employés utilisent les ressources matérielles et logiciels de votre réseau et pouvez intervenir au bon moment;
- Un meilleur contrôle des accès internet : qui accède à des sites non productifs – pornographie, Facebook, Instagram, etc. – et à quelle fréquence;
- De savoir si vos télétravailleurs sont vraiment branchés comme convenu et à quels fichiers ils ont accédés.

4) Outil de contrôle financier

Le SIEM permet de limiter les **dommages financiers, le déficit d'image de marque ainsi que les impacts sur les opérations, les clients et les employés**.

Dans un contexte où **la majorité des entreprises ont d'importants défis de recrutement et doivent fonctionner à ressources réduites**, le SIEM amène l'assurance d'identifier rapidement des menaces et de réduire le délai de réaction. En accélérant l'identification et l'analyse des événements de sécurité, il atténue les conséquences d'attaques et facilite la restauration qui s'ensuit.

Un SIEM s'avère capable de **détecter des incidents de sécurité qui seraient passés inaperçus et d'en identifier précisément l'origine** afin de mettre en place un plan correctif et préventif plus efficace :

- Détection d'attaques de logiciels malveillants tels que virus et **Ransomware**;
- Vol d'information sensible;

- Trafic anormal sur le réseau, transfert de données non autorisé, par exemple : informations sensibles envoyée à l'extérieur vers des sites douteux en Chine, Russie, etc.;
- Destruction d'information sensible par un employé ou un externe tel que listes de clients;
- Exfiltration de données, par exemple copie de données sur clé USB;
- Mauvaises configurations favorisant une faille de sécurité, par exemple le système de caméra envoie des informations non autorisées à l'extérieur;
- Perte de productivité par consommation des réseaux sociaux ou autres sites non productifs
vol de temps : LinkedIn, Facebook, Indeed, Jobillico.

Anticipation de pannes

Le SIEM permet donc une **meilleure anticipation** des incidents aux prémices d'une attaque d'envergure et de remonter à la source de vos problèmes de sécurité **AVANT** que vos équipements ne tombent en panne. **Vous évitez donc les temps d'arrêts coûteux associés aux failles:**

- En détectant des logiciels malicieux ou non autorisés installés sur le réseau
- En interceptant des tentatives d'intrusions et les attaques

On met l'intelligence artificielle au service de la détection de pannes.

Selon une étude approfondie menée par Osterman Research, 87 % des employés qui partent emportent des données avec eux. Que font-ils avec cette information? Ils l'utilisent dans leur prochain emploi chez votre concurrent, la vendent à des concurrents ou deviennent un concurrent.

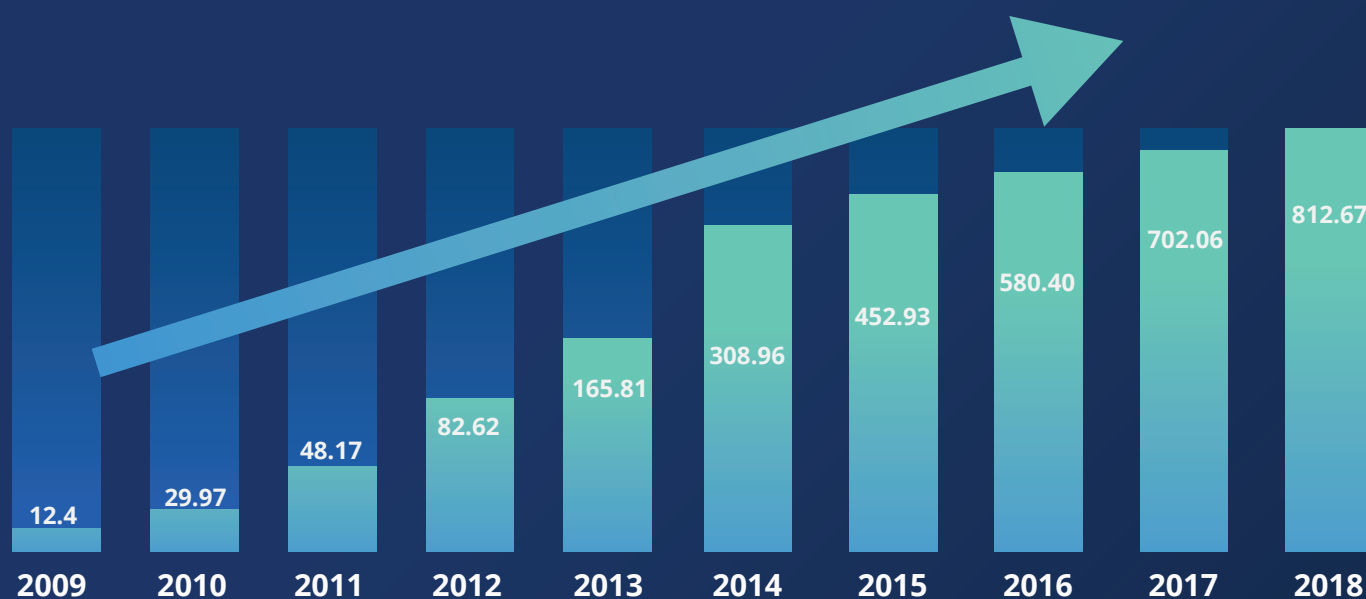
Réduction des coûts d'assurance en cybersécurité

Un bon contrôle par le SIEM aide à réduire les coûts d'assurance en cybersécurité. L'évaluation de vos cyber-risques est en fonction des menaces émergentes et d'autres variables en évolution. De par le SIEM, le rapport de risques et de menaces aide à anticiper ces menaces et permet de mettre en place un plan correctif et d'amélioration continue.

Le SIEM, un outil à l'ère de son temps

L'impact positif du SIEM sur les affaires de l'entreprise le positionne aujourd'hui comme un allié indispensable dans la conjoncture actuelle. Il devient un outil de gestion pour **la haute direction qui doit désormais prendre pleinement part à la gouvernance de la sécurité globale de l'organisation, en équipe avec son département des TI**, afin d'en assurer la viabilité financière et de veiller à ce que les **intérêts des actionnaires, des clients et des employés soient protégés.**

ANNEXE A – STATISTIQUES

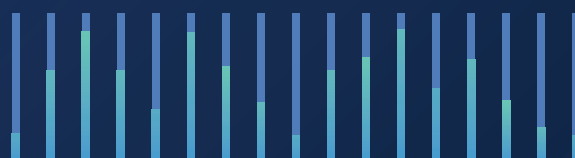


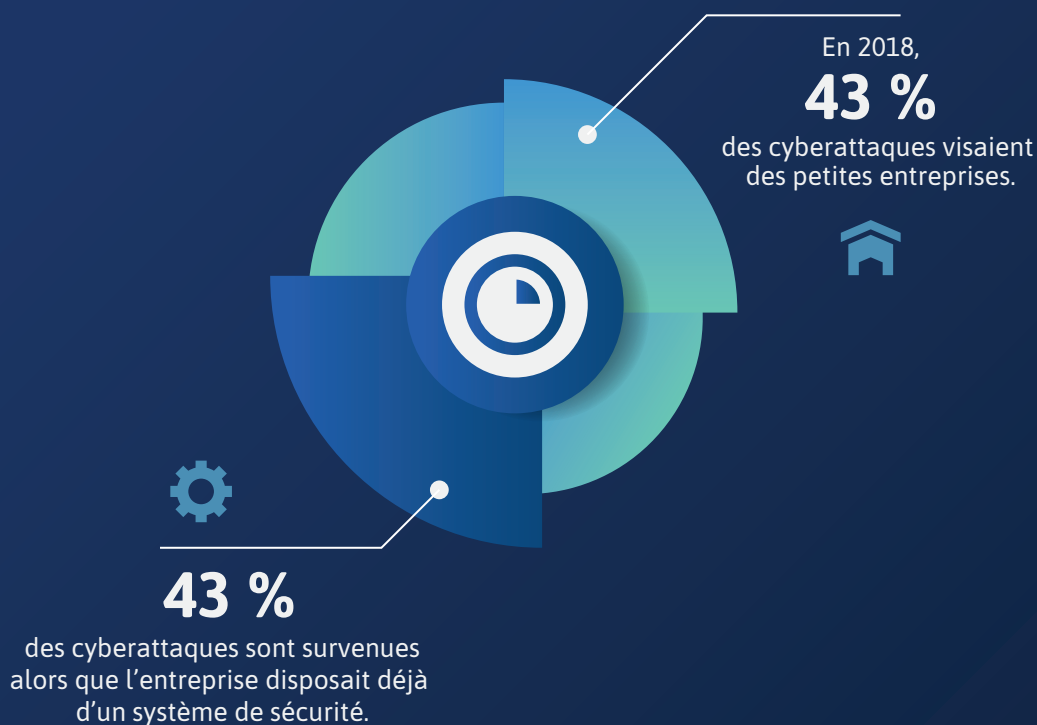
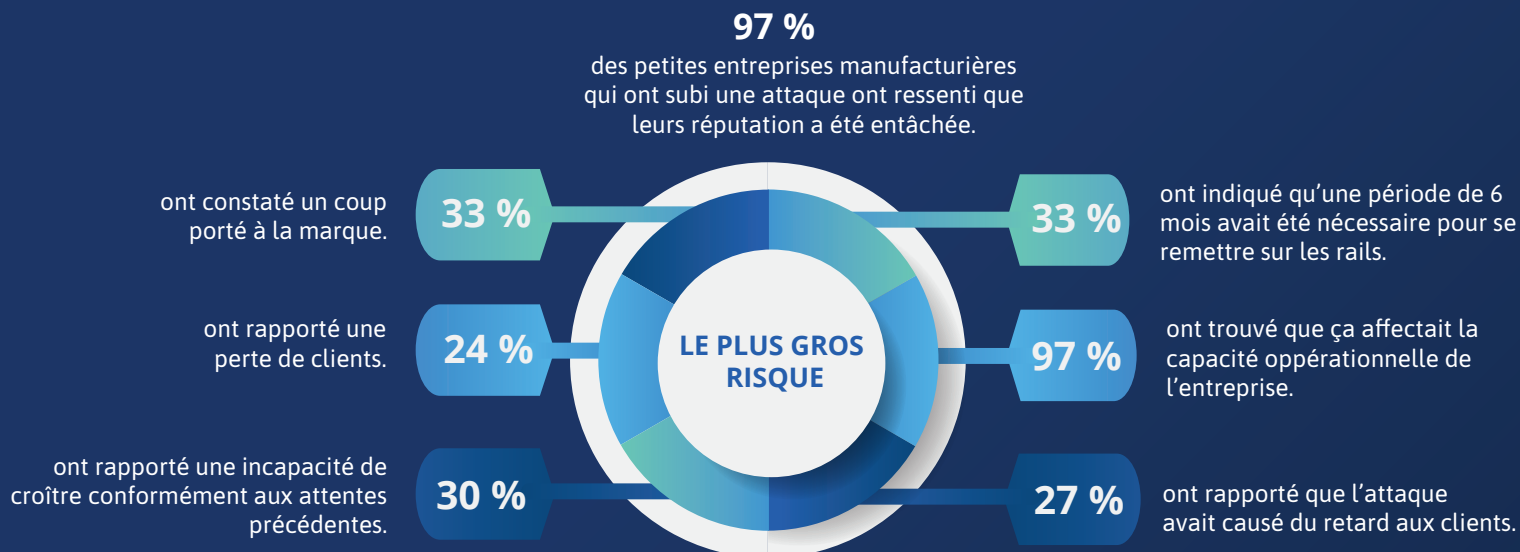
Taux de croissance des infections liées aux logiciels malveillants (en millions)

LE SECTEUR MANUFACTURIER

« De nos jours, la majorité des systèmes manufacturiers sont conçus pour être productifs,
— ils ne sont pas conçus pour être sécuritaires. Chaque manufacturier cours un risque.
— Il n'est plus question de se demander si une attaque va survenir mais de se demander quand elle va survenir. »

Rebecca Taylor, Vice-Présidente Senior
Centre National des Sciences Manufacturières





ANNEXE B - RAPPORTS

Liste des modifications aux groupes octroyant des accès sensibles

☐	Collection Time	Event Type	Log Collector	Serveur affecté	Utilisateur	Groupe touché	Description de l'activité	Résultante
☐	2019-11-13T13:45:06	Log			Louis Fequet	GSG_DEL_Remote_Assistance	A member was added to a security-enabled global group.	Success
☐	2019-11-13T13:45:06	Log			Gabriel Couture-Poulin	GSG_DEL_Remote_Assistance	A member was added to a security-enabled global group.	Success
☐	2019-11-13T15:18:26	Log			567	G_A_Creo_Ordinateur	A member was added to a security-enabled global group.	Success
☐	2019-11-13T16:40:16	Log			Marie-Eve Boucher	SSL_QC	A member was added to a security-enabled global group.	Success
☐	2019-11-14T11:16:04	Log			Jason Beaulieu	GSG_DEL_Admin_SRV-QC-APP04	A member was added to a security-enabled global group.	Success
☐	2019-11-14T11:49:11	Log			Jason Beaulieu	GSG_DEL_Niv1_SRV-QC-FIC01	A member was added to a security-enabled global group.	Success
☐	2019-11-14T13:55:53	Log			568	G_A_Creo_Ordinateur	A member was added to a security-enabled global group.	Success

Anomalies d'ouverture de session ou tentative d'intrusion par un service

Profile PreQuery: lc.cid contains logon.type = '8' || logon.type = '9'

☐	Collection Time	Event Type	Serveur affecté	Description de l'événement	Résultante	Utilisateur ouvrant la connexion	8 = RDP, 7 = RunAs	Résultat	Code de résultat	Category
☐	2019-11-13T11:54:02	Log		An account failed to log on.	Failure	danielb	8	Unknown user name or bad password.	0xc000006d	Logon
☐	2019-11-13T17:35:55	Log		An account failed to log on.	Failure	patrick.letourneau@ars-solutions.ca	8	Unknown user name or bad password.	0xc000006d	Logon
☐	2019-11-13T17:35:55	Log		An account failed to log on.	Failure	patrick.letourneau@ars-solutions.ca	8	Unknown user name or bad password.	0xc000006d	Logon
☐	2019-11-13T17:45:04	Log		An account failed to log on.	Failure	nicolasv	8	Unknown user name or bad password.	0xc000006d	Logon
☐	2019-11-13T20:44:46	Log		An account failed to log on.	Failure	renee.blouin@ars-solutions.ca	8	Unknown user name or bad password.	0xc000006d	Logon
☐	2019-11-13T20:44:46	Log		An account failed to log on.	Failure	renee.blouin@ars-solutions.ca	8	Unknown user name or bad password.	0xc000006d	Logon
☐	2019-11-14T09:23:44	Log		An account failed to log on.	Failure	michelg	8	Unknown user name or bad password.	0xc000006d	Logon
☐	2019-11-14T09:23:44	Log		An account failed to log on.	Failure	michelg	8	Unknown user name or bad password.	0xc000006d	Logon
☐	2019-11-14T09:23:44	Log		An account failed to log on.	Failure	michelg	8	Unknown user name or bad password.	0xc000006d	Logon
☐	2019-11-14T09:23:44	Log		An account failed to log on.	Failure	michelg	8	Unknown user name or bad password.	0xc000006d	Logon
☐	2019-11-14T09:23:44	Log		An account failed to log on.	Failure	michelg	8	Unknown user name or bad password.	0xc000006d	Logon

Trafic réseau vers ou à partir d'entités contrôlées par le crime organisé

	Source City (5 values)	
	mainpuri (161) - karachi (8) - tallinn (8) - shanghai (3) - delhi (1)	
	Source Country (10 values)	
	netherlands (4,162) - russia (1,033) - russian federation (945) - india (162) - bulgaria (130) - turkey (126) - estonia (31) - united states (18) - pakistan (11) - china (3)	
	Source IP Address (20 values)	
	81.22.45.39 (496) - 185.143.223.122 (442) - 185.143.223.150 (441) - 185.143.223.134 (436) - 185.143.223.151 (404) - 185.143.223.114 (400) - 185.143.223.112 (393) - 185.143.223.118 (390) - 185.143.223.139 (385) - 185.143.223.135 (375) - 185.143.223.137 (370) - 81.22.45.85 (175) - 81.22.45.159 (168) - 103.100.168.230 (161) - 45.139.200.133 (126) - 193.32.163.44 (70) - 193.32.163.123 (52) - 185.143.221.62 (41) - 81.22.45.74 (24) - 185.53.88.75 (24) ... show more	
	Source Organization (11 values)	
	information technologies llc (4,078) - infolink llc (903) - broban internet services pvt (161) - ip donner oleg alexeevich ltd (130) - cloud star hosting services (61) - estoxy ou (23) - xns technology group (18) - ebone network (pvt) ltd (8) - fiber grid inc (8) - shanghai telecom science & technology development (3) - ani network pvt (1)	
	Subject	
	Closed - Click to Open	
	Threat Category (1 value)	
	suspect (5,524)	
	Threat Description (14 values)	
	sbl420772 (4,036) - sbl438250 (903) - sbl456874 (161) - sbl438244 (130) - sbl459286 (126) - sbl438242 (61) - sbl420774 (43) - sbl438248 (23) - sbl461359 (18) - sbl175056 (8) - sbl458210 (8) - sbl315954 (3) - sbl381930 (3) - sbl458231 (1)	
	Threat Source (2 values)	
	spamhaus_edrop_list_ip (5,199) - spamhaus_drop_list_ip (325)	
	Time (20 values)	
	2019-11-15T01:11:00 (34) - 2019-11-15T05:10:00 (31) - 2019-11-15T01:25:00 (25) - 2019-11-15T02:08:00 (25) - 2019-11-15T02:16:00 (25) - 2019-11-14T18:00:00 (21) - 2019-11-15T01:38:00 (21) - 2019-11-15T02:58:00 (21) - 2019-11-15T00:31:00 (20) - 2019-11-15T03:54:00 (20) - 2019-11-15T07:27:00 (20) - 2019-11-15T01:14:00 (19) - 2019-11-15T01:31:00 (19) - 2019-11-15T01:34:00 (19) - 2019-11-15T02:04:00 (19) - 2019-11-14T18:57:00 (18) - 2019-11-14T19:46:00 (18) - 2019-11-15T02:01:00 (18) - 2019-11-15T06:49:00 (18) - 2019-11-15T00:16:00 (17) ... show more	

Trafic provenant ou allant vers des adresses IP réputées criminelles ou malicieuses

Utilisation de logiciels d'échange d'informations pas nécessairement homologués

	Profile PreQuery: lc.cid =	threat.category = 'data leakage'	not (alias.host contains 'icloud')
2019	11 14	13:27:00 (-05:00)	Last 24 Hours
	Threat Category (1 value)		
	data leakage (67)		
	Threat Source (1 value)		
	netwitness (67)		
	Enablers of Compromise (1 value)		
	file sharing apps (67)		
	Hostname Alias Record (1 value)		
	api.dropbox.com (67)		
	Password		
	Closed - Click to Open		
	Device Type (1 value)		
	fortinet (67)		
	Device IP (1 value)		
	(67)		
	SQL Query		
	Closed - Click to Open		
	Query		
	Closed - Click to Open		

Cas d'espèce où iCloud serait permis mais pas Dropbox

Trafic vers des pays frappés de restrictions où aucune relation d'affaire n'est entretenue

ars-nw-hu - Broker Last 24 Hours Query SML RSA Threat Analysis Actions Incidents

Profile PreQuery: lc.cid country.dst = 'russia' Cancel

Trafic vers la Russie

Collection Time	Event Type	Session Analysis	Service Analysis	File Analysis	Alerts	Source IP Address	Destination IP Ad	Destination Port	Source Country	Destination Country	Destination Domain	Source Organization	Destination Organization	Action Event	Password	Device Type	Device IP
2019-11-14T13:59:27	Log	not top 20 dst	hostname invalid			5.188.210.101			Russia			Petersburg Internet Network Ltd.		ssl-exit-error		fortinet	10.10.1.1
2019-11-14T13:59:39	Log	not top 20 dst	hostname invalid			5.188.210.101			Russia			Petersburg Internet Network Ltd.		ssl-exit-error		fortinet	10.10.1.1
2019-11-14T14:01:38	Log	not top 20 dst	hostname invalid			5.188.210.101			Russia			Petersburg Internet Network Ltd.		ssl-exit-error		fortinet	10.10.1.1
2019-11-14T14:01:43	Log	not top 20 dst	hostname invalid			5.188.210.101			Russia			Petersburg Internet Network Ltd.		ssl-exit-error		fortinet	10.10.1.1
2019-11-14T18:46:54	Log	not top 20 dst				213.180.204...	443	Reserved	Russia		yandex.ru	YANDEX LLC		accept		fortinet	10.10.1.1
2019-11-14T18:47:13	Log	not top 20 dst				87.250.250.2...	443	Reserved	Russia			YANDEX LLC		close		fortinet	10.10.1.1
2019-11-14T18:48:22	Log	not top 20 dst				213.180.204...	443	Reserved	Russia		yandex.ru	YANDEX LLC		close		fortinet	10.10.1.1
2019-11-15T01:50:55	Log	not top 20 dst				37.193.156.1...	123	Reserved	Russia		novotelecom...	Novotelecom Ltd		deny		fortinet	10.10.1.1
2019-11-15T05:46:55	Log	not top 20 dst				178.248.237...	443	Reserved	Russia			HLL LLC		close		fortinet	10.10.1.1
2019-11-15T05:47:49	Log	not top 20 dst				178.248.237...	443	Reserved	Russia			HLL LLC		close		fortinet	10.10.1.1
2019-11-15T05:47:58	Log	not top 20 dst				178.248.237...	443	Reserved	Russia			HLL LLC		close		fortinet	10.10.1.1
2019-11-15T06:00:48	Log	not top 20 dst	hostname invalid			185.156.177...			Russia			LLC SyvazTelecom		ssl-exit-error		fortinet	10.10.1.1
2019-11-15T06:54:04	Log	not top 20 dst				178.248.237...	443	Reserved	Russia			HLL LLC		close		fortinet	10.10.1.1
2019-11-15T07:31:12	Log	not top 20 dst				94.247.111.10	123	Reserved	Russia			CTV-Belovo LLC		deny		fortinet	10.10.1.1
2019-11-15T08:18:45	Log	not top 20 dst				178.248.237...	443	Reserved	Russia			HLL LLC		close		fortinet	10.10.1.1
2019-11-15T09:05:43	Log	not top 20 dst				178.248.237...	443	Reserved	Russia			HLL LLC		client-rst		fortinet	10.10.1.1
2019-11-15T09:06:48	Log	not top 20 dst				178.248.237...	443	Reserved	Russia			HLL LLC		client-rst		fortinet	10.10.1.1
2019-11-15T09:06:48	Log	not top 20 dst				178.248.237...	443	Reserved	Russia			HLL LLC		client-rst		fortinet	10.10.1.1
2019-11-15T09:46:45	Log	not top 20 dst				217.69.139.2...	80	Reserved	Russia		mail.ru	Mail.Ru Services		close		fortinet	10.10.1.1
2019-11-15T11:03:08	Log	not top 20 dst				178.248.237...	443	Reserved	Russia			HLL LLC		close		fortinet	10.10.1.1

Page 1 | 25 events per page

Displaying 1 - 21 of 21 events

Interrogation sur la consommation Internet des utilisateurs (appui aux RH)

Visualization

Feed Description Closed - Click to Open

Feed Name Closed - Click to Open

File Entropy Closed - Click to Open

File Size Closed - Click to Open

Filter (54 values)

information technology (72,762) - advertising (21,158) - business (11,925) - search engines and portals (11,390) - streaming media and download (8,534) - content servers (7,017) - internet radio and tv (6,867) - social networking (5,288) - remote access (4,748) - news and media (4,191) - information and computer security (3,880) - entertainment (2,382) - web analytics (1,891) - finance and banking (1,758) - file sharing and storage (1,511) - shopping (1,476) - freeware and software downloads (1,105) - meaningless content (966) - games (929) - internet telephony (805) - society and lifestyles (498) - reference (469) - health and wellness (455) - instant messaging (388) - web hosting (381) - web-based email (373) - unrated (289) - general organizations (269) - brokerage and trading (259) - sports (250) - travel (241) - online meeting (234) - web-based applications (228) - education (198) - auction (156) - personal vehicles (144) - real estate (126) - government and legal organizations (104) - personal websites and blogs (62) - arts and culture (52) - domain parking (50) - secure websites (47) - alcohol (35) - custom1 (30) - newly observed domain (28) - newsgroups and message boards (22) - job search (18) - child education (16) - lingerie and swimsuit (10) - global religion (6) - medicine (5) - web chat (5) - restaurant and dining (4) - dynamic content (2)

Full Name Closed - Click to Open

Hostname Alias Record (20 values)

r1--sn-8qu-t0a6.googlevideo.com (8,623) - tlu.dl.delivery.mp.microsoft.com (6,830) - settings-win.data.microsoft.com (5,391) - v10.events.data.microsoft.com (5,175) - apl.radio.net (4,788) - us-njc-anx-r010.teamviewer.com (4,547) - www.facebook.com (4,438) - ctldl.windowsupdate.com (4,177) - crl.microsoft.com (3,875) - www.google.com (3,875) - cp601.prod.do.dsp.mp.microsoft.com (3,388) - safebrowsing.googleapis.com (2,958) - 11.tlu.dl.delivery.mp.microsoft.com (2,923) - www.meteormedia.com (2,734) - 2.tlu.dl.delivery.mp.microsoft.com (2,666) - fonts.gstatic.com (2,492) - disc601.prod.do.dsp.mp.microsoft.com (2,450) - lb.adnxs.com (2,405) - clients4.google.com (2,361) - array607.prod.do.dsp.mp.microsoft.com (2,327) ... show more

IP Address Closed - Click to Open

Utilisation d'Internet par utilisateur (en particulier lorsque FSSO est actif chez le client, mais d'autres technologies sont possibles)

Utilisation d'outils de prise de contrôle à distance non autorisés

Profile PreQuery: lc.cid = risk.suspicious contains 'tunneling'

2019 11 14 13:27:00 (-05:00) BU : Last 24 Hours

- Action Event** (3 values)
fw:outbound-network-traffic (3) - pass (2) - passthrough (1)
- Alert ID** (2 values)
fw:categories (3) - nw110075 (3)
- All Analysis Keys** (2 values)
not top 20 dst (3) - tunneling remote control client website (3)
- All Hostname Keys** (1 value)
update-check.realvnc.com (3)
- All IPv4 Keys** (4 values)
(3) - 146.101.60.86 (3) - (3) - (3)
- Bytes Received**
Closed - Click to Open
- Bytes Sent**
Closed - Click to Open
- Category** (3 values)
"app-ctrl" eventtype="app-ctrl-all" (2) - network.service (2) - "webfilter" eventtype="ftgd_allow" (1)
- Certificate Checksum**
Closed - Click to Open

Trafic généré par le 'ping' de mise à jour d'un logiciel de prise en contrôle à distance non-nécessairement autorisé par la gouvernance.

Chronologie de connexions/déconnexions au VPN (présence des télétravailleurs)

☐	Date et heure	Description de l'activité	Utilisateur ouvra	Résultat	Category
☐	2019-Nov-15 10:17:37.000	SSL tunnel established	juliem()	tunnel established	vpn
☐	2019-Nov-15 10:17:36.000	SSL tunnel established	juliem()	login successfully	vpn
☐	2019-Nov-15 10:19:48.000	SSL tunnel established	joanb	login successfully	vpn
☐	2019-Nov-15 10:19:52.000	SSL tunnel established	joanb	tunnel established	vpn
☐	2019-Nov-15 10:25:37.000	SSL tunnel established	jocelyne	login successfully	vpn
☐	2019-Nov-15 10:25:39.000	SSL tunnel established	jocelyne	tunnel established	vpn
☐	2019-Nov-15 10:26:32.000	SSL tunnel shutdown	jocelyne	User requested termination of service	vpn
☐	2019-Nov-15 10:26:32.000	SSL tunnel shutdown	jocelyne	User requested termination of service	vpn
☐	2019-Nov-15 10:34:52.000	SSL tunnel shutdown	joanb	User requested termination of service	vpn