Comparatif des solutions SIEM / XDR du marché

		SIEM / XDR du marché						SIM	NDR	EDR		
		ITrust Reveelium	Splunk	Elastic SIEM	Logpoint	Qradar et RSA	Sekoia	Elastic Opensource	Darktrace	Tehtris	SentinelOne	Crowdstrike
Editeur	Nationalité HQ	🇫🇷	🇺🇸	🇺🇸	🇩🇰 🇺🇸 🇩🇪 🇨🇳	🇺🇸	🇫🇷	🇺🇸	🇺🇸	🇫🇷 🇫🇷 🇺🇸	🇺🇸	🇺🇸
	Actionnaires majoritaires	🇫🇷	🇺🇸	🇺🇸	🇺🇸	🇺🇸	🇫🇷	🇺🇸	🇺🇸	🇫🇷	🇺🇸	🇺🇸
	Equipe R&D principale	🇫🇷	🇺🇸	🇺🇸	🇨🇳	🇺🇸	🇫🇷	🇺🇸	🇬🇧	🇫🇷	🇺🇸	🇺🇸
	Année de création	2007					2022					
	Cible	Professionnelle	Professionnelle	Professionnelle	ETI	Professionnelle	PME ETI	PME ETI	Professionnelle	Professionnelle	Professionnelle	Professionnelle
	Technologie	SIEM XDR UEBA (logs)	SIEM (logs)	SIEM (logs)	SIEM (logs)	SIEM (logs)	SIM Threat intel (logs)	SIM (logs)	Sonde NDR	EDR	EDR	EDR
	Base de données	Elastic	Splunk	Elastic	Elastic	IBM	Elastic	Elastic	Inconnue	Wazuh	N/A	N/A
	Impact sur l'infrastructure (Agents, sonde, etc...)	Pas d'impact	Pas d'impact	Pas d'impact	Pas d'impact	Pas d'impact	Pas d'impact	Pas d'impact	impact lourd	impact lourd	impact lourd	impact lourd
Déploiement	Déploiement											
	On Premise	OUI					NON					
	Saas Cloud dédié						Partiel					Partiel
	Hybride											
	Saas Cloud Mutualisé - Multitenant		Partiel									
	Parseurs et connecteurs	OUI					Partiel	Partiel	Partiel	Partiel	Partiel	Partiel
	Nécessite un agent local	Non	Non	Non	Non	Non	Rsyslog	Non	une Sonde	un Agent	un Agent	un Agent
	Temps d'installation et paramétrage	quelsques heures	des semaines	des jours	des jours	des semaines	des jours	des jours	des jours	des jours	des jours	des jours
	Tarification maitrisée et fixe		Non	Non								
	Tarification selon	à l'IP ou à la taille de l'entreprise	à l'EPS et IP	à l'EPS et IP	Au Nœud	au moteur, au hardware, aux IP	à l'ip		selon le nombre de sondes / à l'IP	au endpoint	au endpoint	au endpoint
	Défense en profondeur (Doctrine moderne)						Partiel			Partiel	Partiel	Partiel
	Support facile et de proximité											Partiel
	Possibilité de le faire manager par l'éditeur			Partiel								
	Reporting de conformité règlementaire								Partiel			
Capacités	Moteur de détection :											
	Détection Sigma									Partiel	Partiel	Partiel
	Corrélation				Partiel							
	Pattern											
	Threat Intelligence, UEBA				Partiel				Partiel			
	Machine Learning			Partiel	En développement							
	SOAR et Workflow menaces											
	Tableaux de bord personnalisables											
	Playbooks											
	Utilisation de la matrice MITRE de référence											
	Solution souveraine non soumise au Patriot Act et Cloud Act											
	Uses cases métiers / Analyse cyber métier											
	Rapports et KPI sur étagère											
	Scanner de vulnérabilité intégré sur étagère											
Labels et Certifications	Mises à jour automatiques											
	Ne nécessite pas d'expertise particulière											
	Confidentialitié des résultats											
	Produit labellisé france Cybersécurité											
	Produit fabriqué en France											
	Entreprise labelisée ANSSI											
	Labelisé utilisé par les armées françaises											