BOMGAR Conformité avec les normes et règlementations

	BESOIN	RÉPONSE BOMGAR	PRODUIT			CIS	PCI	NIST	HIPPA	ISO	NERC	CJIS	FFIEC	RGPD
	En matière d'accès à distance sécurisé, les règlementations visent à garantir que les données sont protégées et aident à limiter les risques de compromissions. Bomgar peut vous aider à respecter les normes en vigueur grâce à ses solutions d'accès sécurisés.		RS	PAM	VT	CSC	3.2	800-53		27001	v5, v6	5.5	Outil d'évaluation de la cybersécurité	
PROTECTION DES COMPTES	Assigner uniquement une fonction primaire par serveur et activer uniquement un seul service, protocole, programme etc. tel que demandé pour le bon fonctionnement du système.	Bomgar propose des solutions sous forme d'appliances avec uniquement les services et protocoles requis par l'application Bomgar.	●	●			2.2.1-2.2.2	CM-7, SA-4, SA-9, SA-15, SC-41					Domaine 3	
	Interdire l'accès aux utilisateurs non-autorisés et garantir une authentification adaptée pour les utilisateurs.	Bomgar propose l'authentification à deux facteurs via RADIUS, Smart Cards ou Bomgar Verify. L'utilisateur peut ainsi s'identifier en utilisant l'appareil de son choix, tel que son téléphone portable ou son ordinateur.	●	●	●		8.3	IA-5, IA-6, IA-8, IA-10, IA-11, MA-4, SC-37	164.308(3) (i)	A9.2.2, A9.4.1	CIP-004-6, Part 3.1			Article 5, Article 25, Article 32
	Définir, mettre en place et gérer (traçabilité, rapport, correction) le paramétrage de sécurité des appareils sur l'infrastructure réseau en respectant une gestion rigoureuse de la configuration et modifier les procédés de contrôle afin d'empêcher les cybercriminels d'exploiter les services et paramètres vulnérables.	Les rapports syslog alertent les administrateurs en cas de changement sur l'appliance Bomgar. Etablissez des procédures de rotation automatique de comptes de service.	●	●	●	11	2.2, 4.1, 6.2	AC-4, CA-3, CA-7, CA-9, CM-2, CM-3, CM-5, CM-6, CM-8, MA-4, SC-24, SI-4		A.9.1.2, A.13.1.1, A.13.1.3	CIP-005-5 R1, CIP-007-5 R2	3	Domaine 3	
	Mettre en place des procédures pour le stockage, la création, le changement et la sauvegarde des mots de passe.	Les administrateurs peuvent créer des profils prestataires et utilisateurs avec des permissions spécifiques. Les mots de passe sont automatiquement générés, contrôlés et réinitialisés selon les paramètres en vigueur. Les administrateurs peuvent fixer des prérequis pour la création de mots de passe (complexité, longueur etc.) et la fréquence de modification. Tous les identifiants sont stockés dans une base de données chiffrée, et ne sont disponibles qu'auprès des utilisateurs autorisés, manuellement via l'interface web ou lorsque cela est programmé via le Gestionnaire de Sessions Privilégiées.	●	●	●	1		IA-5	164.308(iii) (D)	A9.3.1, A9.4.2, A9.4.3	CIP-004-6, Part 4.1 and 4.3			
CONTRÔLE DES COMPTES	Tracer, contrôler, gérer et modifier l'utilisation, l'attribution et la configuration de privilèges sur les postes de travail, réseaux et applications.	Bomgar offre la possibilité d'attribuer des accès et droits granulaires et tous les flux passent par des ports standards. Les administrateurs peuvent définir des permissions de session granulaires et configurer des paramètres tels que les périodes et zones d'accès. Les accès peuvent également être approuvés au cas par cas. Les sessions prennent fin automatiquement à la fin de la période spécifiée. Les administrateurs peuvent configurer des Jump Clients pour les comptes souvent utilisés et utiliser les protocoles existants dont RDP, Vpro, SSH Telnet, SUDO etc. Chaque accès peut être enregistré pour faciliter les audits.	●	●	●	5, 14	2.1, 7.1-7.2, 8.1-8.3, 8.7	AC-2, AC-6, AC-17, AC-19, CA-7, IA-4, IA-5, SI-4	164.310(b), 164.310(c), 164.412 (A) (1), 164.308(3) (c), 164.312 (2) (i)	A.9.1.1, A.9.2.2-A.9.2.6, A.9.3.1, A.9.4.1-A.9.4.4	CIP-004-5 R4, CIP-004-5 R5, CIP-007-5, R5, CIP 004-6, R5	4 (4.2, 4.3)	Domaine 3	
	Gérer (traçabilité, contrôle et correction) l'utilisation de ports, protocoles et services sur les appareils en réseau afin de limiter la surface d'attaques.		●	●		9		CM-7, SA-4, SA-9, SA-15, SC-41				3		
	Gérer (inventaire, traçabilité et correction) les appareils sur le réseau pour que seuls les appareils autorisés aient un accès, et identifier les appareils non-autorisés et non-gérés pour le leur interdire.	Bomgar permet aux admins de gérer la rotation et le stockage des identifiants, de contrôler, ajouter ou supprimer les IDs d'identifiants facilement sans exposer les mots de passe en clair, de mettre en place des politiques de mots de passe et des permissions pour que les utilisateurs puissent modifier leurs mots de passe dans un temps donné. Les comptes utilisateurs peuvent être intégrés à un Active Directory ou d'autres comptes LDAP pour simplifier leur création ou suppression, et la gestion des permissions. Bomgar permet de supprimer l'utilisation de VPN comme méthode d'accès aux fournisseurs et prestataires.	●	●		16		PE-5, CM-8						
	Gérer le cycle de vie des comptes du système et des applications (création, utilisation, inactivité, suppression) afin de réduire le périmètre d'attaques des cybercriminels.		●	●	●		8.2.1, 8.2.3, 8.2.4, 8.2.5, 8.2.6	AC-2, AC-6, IA-2, IA-5	164.308 (5) (D)					
	Attribuer à tous les utilisateurs un identifiant unique avant de leur accorder un accès aux systèmes et données critiques, et contrôler l'ajout, la suppression et la modification de ces identifiants.	Les IDs uniques des utilisateurs peuvent être configurés manuellement ou être intégrés à un répertoire existant tel que Microsoft Active Directory, Open LDAP ou RADIUS.	●	●	●		8.1.1, 8.1.2, 8.1.3	AC-5, IA-2, PS-4	164.312 (a) (2)(i)				Domaine 3	
ANALYSE ET CONTRÔLE DES DONNÉES	Acquérir, évaluer et prendre des mesures nécessaires afin d'identifier les vulnérabilités, et réduire la surface d'attaques des cybercriminels.	L'activité d'une session est automatiquement enregistrée et listée. Les utilisateurs peuvent générer des rapports détaillés. Bomgar peut s'intégrer avec les outils SIEM pour des analyses détaillées de journaux de logs. Il est également possible de configurer des alertes en cas d'activités inappropriées ou suspicieuses. Les sessions peuvent être autorisées au cas par cas et les protocoles configurés via des outils de gestion du changement. Les accès peuvent être granulaires. La rotation des identifiants dès la fin de la session garantit l'optimisation des identifiants disponibles. Les solutions Bomgar peuvent être intégrées à un outil SIEM pour renforcer la stratégie de sécurité en profondeur.	●	●	●	4		CA-2, RA-4, SA-11, SA-12, SA-15, SC-38, SI-2, SI-4, SI-5	164.308(1) (D)	6	CIPP-007-5 R2, CIP-010-5 R3	10		
	Empêcher l'exfiltration de données, limiter ses conséquences et garantir la protection et l'intégrité des données sensibles.		●	●		13	10.5	SC-7, SC-8, SC-16, SC-28, SC-34, SI-1, SI-4, SI-7, SI-10, PE-3	164.310 (a)(1)	A.18.1.4	CIPP-011-5 R1	3	Domaine 3 Domaine 5	
	Collecter, gérer et analyser les journaux d'évènements et d'activités pour détecter et comprendre une attaque et recouvrer l'état des données et du système. Ces journaux doivent indiquer les informations d'identification de l'utilisateur, le type d'activité, la date et le lieu.		●	●		6	10.1, 10.2, 10.2.2, 10.2.3, 10.2.4, 10.3	AU-2, AU-3, AU-6, AU-7, AU-14	164.308 (5)(C)	A12.4.1, A12.4.3		4		
	Mettre en place des procédures pour contrôler les tentatives de connexion et signaler les anomalies.		●	●				AC-7	164.308 (5)(C)	A12.4.2	CIPP-005-3 R3, CIPP-007-3 R5, CIPP-007-3 R6	10	Domaine 3	
	Organiser des évaluations régulières afin d'identifier les menaces malware. S'assurer que tous les composants et logiciels du système sont protégés des vulnérabilités identifiées et installer des patchs de sécurité sous 30 jours à partir de leur date de disponibilité.	Bomgar effectue des analyses de vulnérabilité régulièrement et mandate des sociétés externes indépendantes pour réaliser des tests d'intrusion, des analyses statiques du produit et est à l'écoute d'évaluations proposées par ses clients. Les patchs de sécurité et de résolution de bugs sont mis à disposition dès que nécessaire.	●	●	●	8	5.1, 5.2, 6.2	AT-3, CA-2, IR-10, MA-3, MA-4, SC-19, SC-26, SC-35, SI-3,	164.308(a) (S), 164.310(d) (I), 164.310(b), 164.310©	AA.8.3.12, A.12.2.1, A.13.2.3	CIPP-007-5 R3	10	Domaine 3	

PRODUITS : **RS** = Remote Support | **PAM** = Privileged Access Management | **VT** = Vault