Creme Global

Data Foundry & Expert Models Platform Security and Service Continuity Details

Creme Global
4th Floor, The Design Tower
Trinity Technology & Enterprise Campus
Grand Canal Quay, Dublin 2, Ireland
Phone: +353 1 677 0071
Email: info@cremeglobal.com
Web: www.cremeglobal.com

Do you hold ISO 27001/2 certification? Are all services offered in the scope of this certification?

All of our services are deployed on Amazon's Web Services, which are all ISO 27001/2 accredited. However, Creme Global itself does not maintain this certification. The full AWS certification can be found here. http://aws.amazon.com/compliance/iso-27001-faqs/

What practices are followed to keep the applications safe?

All users are invited on to the system. When users log in for the first time they are asked to change passwords. User passwords use PBKDF2 (Password-Based Key Derivation Function 2). The API uses good restful practices, including authentication per request. All communication with the Expert Models web app is via 256-bit encryption.

What is the process for inviting a user into the system?

To add a user to the system a group coordinator, that is known to the Creme Global project coordinator, sends a request including an email address to the Creme Global project coordinator. That user is sent a link which when clicked will bring them to a page to set an initial password to associate with their email address.

Is there Antivirus software on the server?

Executables cannot be installed on the Expert Models platform. Creme Global use webroot antivirus on all team personnel Windows PCs.

What Firewalls are in use?

AWS server access is restricted to the Creme Global Office (or from home to the office via a VPN) the office systems are protected by an IDS (config server).

Is there penetration and vulnerability checking?

There are automatic daily updates for the operational system's security software, constant monitoring of system files' integrity using rkhunter and server access locked within the office's VPN.

Are there any safe coding practices you use?

Good safe coding is expected of all Creme Global software engineers. On the Expert Models platform, some of these include:

- Validate Input; Only a limited type of data can be upload to the system and all this data is validated. Head compiler warnings; We take compiler warnings very seriously.
- Security architecture; We separate functions on separate nodes with secure connections, such as web node and compute node. Keep it simple; A key aspect our gatekeepers look for during code reviews is that the architecture and functions are as simple as possible.
- The principle of least privilege; There are many layers of access to our systems and they are granted on an as needs basis for least privilege.

We have a distinct QA function in our company that takes security as part of the cycle.

Provide details of the patch management procedure followed

All software is stored and versioned with Git. The bug fixing process involves creating a bug fix branch and merging that branch back to development and QA. From QA it can be released. but that bug fix is also carried forward to future releases. Patches are released from QA on an as required basis, release notes detailing everything that has been altered are generated from our ticketing and release management system JIRA.

Details on the EC2 instance maintenance and patching procedure are documented at https://aws.amazon.com/maintenance-help/.

In the event of resource overload (processing, memory, storage, network) what information is given about the relative priority assigned to our request in the event of a failure in provisioning? Is there a lead time on service levels and changes in requirements?

All services are hosted on the same instances. So return to service for all our users will be our number one priority. Great care has been taken in the design of the system and the selection of the service providers (see below) to ensure resource overloading is not an issue.

How much can you scale up? Do you offer guarantees on the availability of supplementary resources within a minimum period?

Our production services are hosted on Amazon Web services, using Elastic Beanstalk to manage EC2 instances. Elastic Beanstalk will continue to create instances to meet demand. AWS provides an uptime guarantee of 99.95%. Our databases are hosted on AWS RDS instances, with monitoring and the ability to scale disk size.

How are the accounts authenticated and managed? How are activities logged? Are these logs being reviewed? Are the admin accounts shared accounts or individual accounts?

All accounts are managed the same way, different roles are assigned to accounts depending on whether they are users or administrators. Accounts are grouped by company, users within a company have a shared area that let them interact and share files, but no other companies have access to any user's information. All users' logins are recorded and these logs are reviewed regularly for security and service optimisation. Admin accounts are individual.

Do administrators maintain separate user accounts for performing specific job functions not requiring administrator rights?

No. Accounts are given a role of administrator, so they can use the same accounts to perform non-administrator tasks (though usually, admins do not perform non-admin tasks).

How often are access rights and privileged reviewed?

When an employee leaves the company their access to the Expert Models platform is revoked. Other reviews of access are carried out infrequently.

How often are activity logs reviewed? What specific activities are being reviewed?

Activity logs are reviewed on a 4-week cycle. The primary goal is to understand users' use of the platform for optimising the user experience, but unusual activity such as excessive admin access will be observed by the product owner.

How are administrator access audited?

When an employee leaves the company their access to admin passwords on LastPass are immediately revoked. Root access to the Expert Models platform is reset every 3 months.

Do Amazon employees have access to your customer data?

Amazon response to this question:
Customers can build sensitive workloads on AWS and we have a wide range of enterprise and government customers doing just that. AWS has demonstrated compliance with FedRAMP, ISO 27001, and PCI, and we also provide a range of SOC audit reports. As a result, there are many government agencies using AWS today to process and store sensitive information. The AWS GovCloud (US) region is an isolated AWS Region designed to allow US government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements.

A few resources for your reference:

- Our Compliance Page, including descriptions of our compliance programs and applicable whitepapers. https://aws.amazon.com/compliance/
- Our Security Page, including information about how we control logical access and how we protect the infrastructure. https://aws.amazon.com/security/

Does Creme Global mean to protect data from being read and copied by the Creme Globals administrators?

Yes, Creme Global administrators and customer support admins have access so they can assist customers when required, but access is restricted to trusted employees.

How do you ensure data cannot be copied by DBAs? Is encryption utilized at the database level and do the DBAs have access to the database master keys?

DBAs do have access to the master keys stored in LastPass. When they connect to the database they can observe customer data and hence copy it.

How are “trusted employees” access determined?

Trusted employees in this context are restricted to admin personnel (in the group previously described). Employees are thoroughly vetted before starting work at Creme Global. Access to the systems is granted only on an as-needed basis.

Please detail the password reset process: e.g. does the password reset process or change procedures include sending passwords by (unencrypted) email?

If a user wishes to reset password they must enter their email, in which case they are sent a link at which they can reset their password. This link can only be used once.

Does the link to the password reset page expire?

In production Expert Models system link the link expires as soon as it is used.

Can the link be forwarded to another user or email address?

We cannot prevent users from forwarding the reset link or indeed their login credentials.

Who could initiate a password reset process?

Anyone can get to the page where the password can be reset, but they must know the email address of the user they wish to reset. The user must then click on a link in their email to get to the password reset page, so in order to complete a password reset process, the person must have access to the email account of the user.

Is the initial password generated automatically?

Users are sent an invite from the platform to their email address. When they click on the personal link in the mail they are asked to set their own password for the platform.

What forms of authentication are used for admin operations?

Only Creme Global administrators have access to the systems on which the Expert Models app executes. This access is carefully controlled. Administrator passwords and ssh keys to AWS services are stored in LastPass and shared only with administrators, passwords are hidden from view. Additionally, we use multifactor authentication to access the AWS console (using a virtual MFA device).

How many users have access to LastPass? What is the process in place when one of the users with LastPass is terminated?

5 trusted Creme employees have access to the admin passwords on LastPass (3 system/support admins, their manager and the CEO). When they leave the company their access to LastPass is revoked and where necessary the quarterly password change is brought forward.

Is two-factor authentication used to manage critical components within the infrastructure, such as firewalls, etc.?

Yes, access to the AWS console requires MFA.

What are the requirements (username, password, pin, etc.) for MFA access?

MFA access uses a virtual token and an IAM account on AWS, set with the following password requirements:

- Must not be the same as your old password
- Must be at least 8 characters long
- Must contain at least one symbol (!@#$%^&*()_+-=[]{}|')
- Must contain at least one number (0-9)
- Must contain at least one uppercase letter (A-Z)
- Must contain at least one lowercase letter (a-z)

Do you support two-factor authentication for client access?

Not currently.

Which password policies do you have in place (minimum requirements)?

Criteria is, 1 uppercase, 1 lowercase, 1 non-alphanumeric and a minimum of 8 characters. Passwords are stored using PBKDF2.

Are there account lockout procedures? Attempts? Duration?

In the production release, after 3 unsuccessful attempts at the password, there is a lockout period of 60 seconds.

Are users able to select their own passwords?

Yes.

How is authentication transported? Is it always encrypted? How are credentials stored within the system/application?

All transportation of credentials is encrypted. Passwords are stored using PBKDF2.

How are the passwords encrypted?

Passwords are encrypted using the Django web framework, using PBKDF2, as described at https://docs.djangoproject.com/en/1.8/topics/auth/passwords/

Are security controls in place for reading and writing encryption keys?

SSH keys for access to systems are controlled and stored in password vault (LastPass) with access granted to only administrators. there is no SSH access to the Expert Models app for end-users.

Are customer system images protected or encrypted?

The Expert Models database is encrypted and hence images of the database are encrypted.

How is it encrypted and what type of encryption?

The data is stored on an AWS RDS instance, the database is encrypted using the AWS encryption option, more details on it can be found at https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html

Who holds the access keys?

Access keys are stored in our password vault. Only Creme Global administrators have access to the production server keys.

Is data in transit, rest and process encrypted? If yes, do DBA's have access to the master decrypt keys?

Data in transit is always encrypted. Database stored on the disk is encrypted, in process, they are not encrypted.

How is the data encrypted?

Data between the browser and the AWS secure VPC uses SHA256 CA – G3. And can be viewed on the site https://app.expertmodels.com Connections are enforced to use SSL.

Are any monitoring tools utilized?

The SSL cert has been verified and can be checked on https://www.digicert.com

What provisions exist in the event of the theft of our credentials (detection, revocation, evidence for actions)?

New credentials can be issued on request.

What is the notification process for events?

If a user notices a breach, they should contact support@cremeglobal.com (which will immediately alert support team).

What steps are taken to determine if credentials were utilized after the event?

All login events and IP addresses are recorded with a timestamp, these can be provided to a customer group in such a case.

Are new credentials issued only on request or automatically upon event reporting?

On any report of a breach, the user's account will be locked while waiting for instructions from the group administrator.

Is there the ability to incorporate single sign-on?

No, not currently.

A user can opt to exit from the platform?

Upon an exit event, all user data can be dumped, returned to the customer and eradicated from our systems. Including users data, user account and user transaction data. As data is backed up regularly, it will be 7 days before all user data is removed from backups.

Will any data be stored on tapes, disks, etc. post contract for a period of time?

The database is encrypted and hence the backups encrypted. The Expert Models backup policy has backups stored for 6 months.

How will the data be returned to the customer?

All data uploaded to the system will be in the user's possession to begin (no primary data is generated using Expert Models).

Are backup tapes encrypted?

Backup is performed via AWS snapshots, the whole encrypted database is stored. Hence the backups are encrypted.

Will data be replicated to different storage locations? If yes, please detail.

Data and backups are all stored in the cloud on AWS services in northern Virginia. These can be backed up to different availability zones on request.

Do you have disaster recovery plans available?

We have moved all services required for the Expert Models system to the cloud and rely on AWSs extremely high disaster prevention measures to mitigate the risk of disaster but also to ensure disaster recovery is a straightforward process of restoring backup images which are collected every day. administrative credentials are also stored in the cloud. Documentation on the recovery actions for the Expert Models platform can be provided on request.

How often do you test disaster recovery and service continuity plans?

Testing recovery of the Expert Models systems is scheduled quarterly.

Do you test the backup and restore procedures? How often?

Backup restoration is tested quarterly.

Is there a real-time security monitoring service in place?

We use Nagios to monitor all of our services, on the Expert Models app we test the Database, the web client and the API. It probes through to get database info, to test for the case that just the webserver is up and the database is not.

Do you provide incident reports of security breaches to customers?

All reports of incidents that affect either the security or site up time for a user will be communicated by email.

Reports on potential customer data leakage will be brought to the customer attention immediately. Where a vulnerability that has the potential to cause a leak occurs, the first priority will be closing the vulnerability. If no resolution is found within an hour the customer will be informed.

What is the process for rectifying vulnerabilities?

Vulnerabilities, when discovered, will be handled on a case by case basis.

We have a dedicated cloud systems administrator who continually monitors all of our services using Nagios along with other tools. He is augmented by two other staff members with a systems administration duty. If a vulnerability is detected by an automated system it will send an email or SMS to the sysadmin group, who will action it immediately. If a vulnerability is discovered by staff or customer it will be triaged by the front line customer support representative who will forward it to tech support.

Do you have an up-to-date virus and malware protection installed on all systems?

It is not possible for users to install executables on our systems.

Is endpoint protection is not installed on all systems?

AWS server access is restricted to the Creme Global office (or via VPN / SSH into the office). Creme Global's servers use Webroot Endpoint Protection. https://www.webroot.com/us/en/business/smb/endpoint-protection

Which prerequisites should be considered that the service could be used? e.g. software versions (Internet browser, Flash, Java, ...)

The Expert Models app is cloud-based. the only requirements are for a modern browser. Browser requirements are Internet Explorer 11 or later, Firefox and Chrome. ActiveX is not used on the Expert Models platform.

What assurance can you provide to us regarding the physical security of the location? Please provide examples and any standards that are adhered to e.g. Section 9 of ISO 27001/2.

AWS complies with extremely high physical security policies including ISO27001. Reference documentation: https://media.amazonwebservices.com/pdf/aws_security_whitepaper.pdf

What environmental controls are in place to protect the data centre?

AWS's data centres are state of the art, utilizing innovative architectural and engineering approaches. See the above document.

Is your infrastructure located in the US or in international locations?

Currently, we support infrastructure in the US in North Virginia and in Dublin, Ireland. Further locations can be considered upon request.

Where will the data be physically located?

It depends on our agreement, it can be stored in either of our standard locations (US, North Virginia or Dublin, Ireland) or alternative locations can be supported upon request.

Is your company safe harbor certified?

Amazon.com, Inc. and its controlled U.S. subsidiaries, including Amazon Web Services, Inc., are participants in the Safe Harbor Program. https://aws.amazon.com/privacy/

Will any of your services be sub-contracted out or outsourced?

All administration of our services is undertaken by direct Creme Global employees.

Creme Global

Creme Global
4th Floor, The Design Tower
Trinity Technology & Enterprise Campus
Grand Canal Quay, Dublin 2, Ireland
Phone: +353 1 677 0071
Email: info@cremeglobal.com
Web: www.cremeglobal.com