Information Security Policy

Information Security is a top priority for Ardoq, and we also rely on the security policies and follow the best practices set forth by AWS.

Procedures will continuously be updated and improved.

1.1 Security policies

Refer to Amazon Web Services Security policy (https://aws.amazon.com/security/) and the shared responsibility model that it's the general principle that AWS is responsible for the security for the cloud services, and Ardoq is responsible for the security within the Application and the setup (https://aws.amazon.com/compliance/shared-responsibility-model/).

Application Security Policy

Ardoq follows Sans Application Security Policy:
https://www.sans.org/security-resources/policies/application-security/pdf/web-application-security-policy

Data Security Policy

- Amazon web console login is protected with two factor authentication, and only available for the few core employees that require that level of access.
- Each customer's data is stored in a separate database, only accessible in the Ardoq application for users belonging to that organization. Direct access to the database is only possible through a dedicated Bastion server with private SSH keys.

Cookies

We use cookies to understand and save your preferences for future visits and it's required for Ardoq's services to work. Other solutions that we integrate with may also use cookies for their services to work.

Cookies are small files that a site or its service provider transfers to your computers hard drive through your Web browser (if you allow) that enables the sites or service providers systems to recognise your browser and capture and remember certain information

How do we protect your information?

We implement a variety of security measures to maintain the safety of your personal information when you place an order or enter, submit, or access your personal information. We offer the use of a secure server. All supplied sensitive/credit information is transmitted via Secure Socket Layer (TSL) technology and then encrypted into our Payment gateway providers database only to be accessible by those authorized with special access rights to such systems, and are required to keep the information confidential. After a transaction, your private information credit cards will be kept on file for more than 60 days in order to pay for monthly subscriptions of the Service.

1.2 External Managed Hosting list of infrastructure locations

Ardoq is hosted on Amazon Web Services data center in Ireland.
It is possible to use other AWS Regions in a dedicated hosting solution.

1.3 Detailed schemes of the technical security measures in place

Application access
All access from the internet to Ardoq is over HTTPS, and goes through an Elastic Load Balancer. Amazon security groups (virtual firewalls) ensure that traffic between the servers only happen on specific ports, both for incoming and outgoing connections. Learn more about Amazon security groups here:
http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html

Server access
Only a few Ardoq employees have access to backend servers. All administration access to Ardoq servers go through a Bastion server. The Bastion server is only accessible when enabled through Amazon AWS Console, and can then be accessed with ssh private keys installed - username/password access is disabled. The private keys are stored in an encrypted vault, and added on the client only when needed.

Amazon AWS access
Only a few Ardoq employees have access to the AWS dashboard. All access requires strong password and two factor authentication.

Ardoq monitors logs from front-end, back-end and database in one centralized Kibana monitoring system. Ardoq also uses Amazon CloudWatch with monitoring and alerts of suspected breaches.

Ardoq has configured AWS security groups, that limit cross component access to the minimum of required ports opened. Apart from this configuration, the firewall setup, maintenance and operation of the firewall is provided by AWS.

Servers are updated and patched regularly.

1.4 External Managed Hosting technical details and additional controls

The current main setup consists of load-balanced redundant front-end Nginx servers, load-balanced redundant API servers, and a cluster of databases. The servers are isolated from each other in separate security groups to increase security.

For monitoring we run a set of monitoring servers with ElasticSearch, Logstash and Kibana. This gives us near real time insight into all requests. (User passwords and session keys are naturally not logged or monitored).

1.5 External Managed Hosting security incident management process

Bounty Program
By invite only - on https://hackerone.com/ardoq.

Server failure
All our servers are monitored using Monit to track performance and availability metrics. We also use Pingdom to track uptime, and alert us of service failure.

Suspected Security breach

1) Shut down bastion server and NAT Gateway. This will make it impossible for anyone to connect to the backend servers, and also terminate any connections from the backend servers to the internet.
2) Create server snapshots of all servers for offline investigation
3) Investigate snapshots for signs of intrusion
4) Search logs for signs of intrusion
5) Involve security team
6) Identify potential breaches

Confirmed Security Breach

1) Shutdown all servers
2) Notify affected customers
3) Create server snapshots for investigation
4) Scan for threats
5) Involve security team
6) Identify root cause
7) Fix root cause
8) Bring systems back online

Alerts
AWS Monitoring is setup to raise alarms for large quantities of data downloaded from Ardoq.

Disaster recovery
All our infrastructure is automated, so completely tearing down and setting up a fresh environment from scratch can be done in a matter of hours, excluding restoring of data.

1.6 External Managed Hosting includes Customers into its incident management process to be notified of collateral events.

All organizations are included in process for serious incidents, regarding both security and downtime. See 1.5.

1.7 External Managed Hosting information about its collateral SLA for hypervisor vulnerability management

Refer to Amazon Web Services Security policy
https://aws.amazon.com/security/

1.8 External Managed Hosting detailed technical specifications of the access management system in place

User Authentication

Ardoq offers two options for user Authentication: i) Username and password ii) OAuth 2.0 Authentication using one of the following Identity provides: Google, Microsoft & Github.

Organizations subscribing to the Premium or Enterprise plan also have the option to use Azure Active Directory as their Identity provider.

Ardoq encourages customers to use OAuth 2.0 Authentication whenever possible. For customers who decided to authenticate using username and password, Ardoq follows industry best-practice for password storage. Passwords are salted and hashed using an adaptive one-way function (bcrypt) with high work factor.

Authorization

Users in Ardoq are authorized to access resources belonging to an organization by being assigned a membership. Users can have membership in multiple organizations, and the level of access is governed by the memberships role within the organization in addition to a set of explicit access controls rights for each workspace.

Ardoq operates with three types of membership roles:
Admin - can edit all data within an organization and invite other members
Writer - can create, edit and delete data within an organization, but not invite other members
Reader - can only read data within an organization

In addition to roles, workspaces in Ardoq are protected by explicit access rights called workspace permissions. For writer roles, workspaces permissions have higher precedence than roles (a writer role might still only be granted read-access on a specific workspace). For reader roles this precedence does not apply (you can't give a reader role edit permissions on a workspace). Assigning rights to a workspace can be done by the user who created the workspace (the owner), or by an admin. Admins have full access to all workspaces in Ardoq, regardless of any workspaces access rights

Request context

Each request to Ardoq is bound to a context which specify the organization the request is trying to access. The context is defined by either a custom domain <organization>.ardoq.com (only available to enterprise plans), via a browser cookie or by a request parameter.

API Authentication

In addition to User Authentication, Ardoq offers a comprehensive REST-api. Users can decided to authenticate API-access using either HTTP Basic Authentication or HTTP Token Based Authentication. All API-access is associated with a user and given the same authorization as that user.

Ardoq encourages customers to use Token Based Authentication when accessing the API. Since separate tokens can be issued for different clients, if one suspect that a token is compromised, the user can delete this token and prevent access to Ardoq while leaving the other tokens active.

1.9 External Managed Hosting technical specifications and controls

All organization data is stored in a separate database. In addition to the master database, the data is replicated to two slave databases.

1.10 External Managed Hosting process and techniques in place for data storage media disposal

Upon customer request, deleting organization data is simply a matter of deleting the database from master and slaves.

Secure deletion of data process:

- Database:
    - Customer data is stored in a separate database, so deletion from the platform is a matter of simply deleting the database.
- Backups:
    - Backups are only kept six months after the backup time. The backups are encrypted and stored in a separate location. Deletion of customer data within the backup is a tedious task, and will be performed on request (billable per hour).

1.11 External Managed Hosting details about the software systems development life cycle (SDLC) policy and procedure in place

Ardoq employs a continuous delivery pipeline. After merging code into master branch it automatically the pipeline builds, tests and deploys a new version of Ardoq. We deploy new features, patches and bug fixes multiple times a day.

Most changes and updates are applied in a rolling fashion, without down-time.

Scheduled down-time is notified in advance to all users via registered email addresses.

Secure Coding Policies

- Ardoq is committed to security by design and secure coding practises. All production code is subject to the following coding policies
    - Code review. All non-trivial changes go through a pull request with one or more persons reviewing the changes with respect to stability, performance, best practises and security.
    - Automated testing (including nightly XSS-testing).
    - Linting. Many security errors originate from bad code. Linting ensures that our code is uniformly formatted, is aligned with coding best practises, and avoid basic mistakes and errors.

- ○ Use of libraries. We use updated, well known and well tested libraries, both in the front end and the back end applications. This reduces the risk of trivial errors like database injection attacks.
- ○ Separate database schemas for organisations: Each organisation has a separate database schema. This makes security checks simple to maintain, and makes data leakage between organisation impossible to do by accident when coding.
- ○ In house development. Our core platform is developed by in house resources following our policies.
- ○ Ardoq follows the above mentioned processes as well as industry established best practices.

1.12 External Managed Hosting information about the software release management and patch management process in place

Ardoq release management follows the SDLC policy. We release features, patches and bug fixes as soon as they are implemented.