Security Log Collection

# Security Log Collection

Ministry of Justice (MoJ) systems and services must adequately create and retain event data as part of the [DETECT](identify-protect-detect-respond-recover.html#detect) portion of the [Cabinet Office's Minimum Cyber Security Standard (MCSS)](https://www.gov.uk/government/publications/the-minimum-cyber-security-standard).

## MoJ Cyber Security Logging Platform

The MoJ Cyber Security team operate a centralised, scalable, multi-tenant, cloud-based log collection and forwarding system for infrastructure (non-application level) log data.

The platform can receive, store, index, filter, search, alert and re-forward log data from any MoJ source (including supplier systems).

## Additive technology supply chain

The security log collection principles are designed to be met through technology supply chain as opposed to each system individually.

For example, where the principles require the logging of DNS traffic, this could be achieved within a corporate device ecosystem by logging at the end user device itself, or by configuring the end user device to use a corporate DNS server that logs instead. You may decide to do both, because some DNS queries can go out without the DNS server (for example in the case of a corporate VPN that is not always on).

Where a platform exists, it should provide some assurance to all its consumers that makes clear what logging it collects and what needs to be logged by its tenants.

For example, if a cloud platform allows you to spin up arbitrary virtual machines, but guarantees that all network traffic must pass via a web proxy to go out, which logs, then the cloud platform can tell you that [Principle 5: Network Events](#network-traffic-events) and [Principle 3: Infrastructure Events](#infrastructure-events) are logged, but that you need to provide [Principle 1. Authentication Events](#authentication-events). The platform may even provide you with a base virtual machine which have logging for authentication events built in, meaning that you don't need to provide any logging at that level.

## Principles

We have created a series of security log collection principle requirements for the MoJ. If you have any questions or comments, [get in touch](cyber-and-technical-security-guidance.html).

To enable ease of referencing, but not to imply priority order, each item is assigned a reference.

### 1. Authentication events

* a: login successes and failures
* b: multi-factor authentication success and failures
* c: logouts
* d: session creation
* e: session timeout/expiry
* f: session close

### 2. Authorisation events

* a: group/role creation, modification or deletion
* b: group/role membership changes (addition or subtraction)
* c: group/role elevation (for example, if a user is able to temporarily assume a higher privilege to conduct a finite amount of work)

### 3. Infrastructure events

Infrastructure is defined as underlying resources, whether a logical switch, server or through to a containerised compute resource in the cloud, upon which end-user or application logic is overlaid.

* a: power/service on / off
* b: creation/registration and deletion/de-registration, including suspension/hibernation if applicable
* c: software update events/status
* e: IP address allocation/deallocation
* f: Firewall/routing rule creation, modification or deletion
* g: Network change events (for example addition or removal of virtual networks or interfaces)

### 4. Domain name service queries

* a: successful and unsuccessful queries
* b: recursive lookup status
* c: infrastructure node / end-user device registration / de-registration (if applicable)

### 5. Network traffic events

* a: successful and unsuccessful inbound service daemon connections
* b: unsuccessful outbound connections where the network traffic is *not* associated to an inbound request

### 6. Contextual security related events

In context and where present, technology may generate events pertinent to security and these must be captured.

For example, operating system patch state information from end-point protection detections through to encryption states within storage arrays.

### 7. Log transmission to the MoJ Cyber Security Logging Platform

* a: All log data must be sent to the MoJ Cyber Security owned log platform unless all principles have already been met through the deployment of a holistic locally deployed and monitored Security Information and Event Management (SIEM) solution.

Where 7(a) above is true, the MoJ Cyber Security team will advise in context what information must be sent from the in-place SIEM to the MoJ Cyber Security Logging Platform.