API Security Requirements Specification - IBM QRadar DMS API

1. Introduction

The IBM QRadar Device Support Module (DSM) API supports event log gathering and normalization across networks and security devices (IBM, 2025). Within a large data infrastructure such as a Security Information and Event Management (SIEM) solution, the DSM API delivers a connector between sources of data and analytic modules. Due to the DSM API’s handling of potentially sensitive operational data, it must be developed with a high level of confidentiality, integrity, and availability (NIST, 2023).

2. Security threats and primary risks

* Impersonation of a third party using the API or token
* Interfering with information during transmission
* SQL injection attacks (leads to data tampering/loss)
* Malicious excessive request rates resulting in denial of service (e.g. DDoS)
* Sensitive data leakage through erroneous responses and/or logs

3. Security Requirements

Transport & Network Security

* The API must enforce HTTPS (TLS 1.2+) on all incoming and outgoing connections.
* Mutual TLS (mTLS) must be enabled for services that are linked with the parser; certificates must be rotated at least once every 90 days (OWASP, 2023).

Authentication and Authorization

* Access must require OAuth 2.0 bearer tokens with well-established scopes; all such tokens will expire after 60 minutes.
* System security controls - Role-based access control (RBAC) must limit DSM functions accesses based on “least-privilege principles”.
* Credentials and secrets must be stored in IBM Secrets Manager or a secured vault, but never hard-coded (IBM, 2025).

Data Validation and Integrity

* All log payloads must be validated against the DSM schema for protection against SQL injection or parser attacks.
* The API must sanitize all input and reject unknown or poorly constructed fields (OWASP, 2023).

Rate Limiting and Availability

* Quotas requested must limit every client to less than 100 requests per minute, returning HTTP 429 when exceeded.
* Timeouts, retries, and circuit breakers must ensure graceful degradation underload.

Monitoring and Logging

* Auditing of authentication attempts, accesses, and failures along with request IDs must be maintained.
* Logs must exclude sensitive payload data and be preserved for 180 days inside the QRadar SIEM for anomaly detection (IBM, 2025).

Data Protection amd Privacy

* Login information with IDs should be AES-256-encrypted at rest and masked when being transmitted externally.
* Data retention periods must comply with GDPR Article 5 (1)(e) and internal policies (e.g., ≤ 90 days) (NIST, 2023)

Versioning and change control

* The API must abide by semantic versioning and must provide at least 90 days’ warning prior to deprecation.
* CI/CD pipelines must conduct static and dynamic security testing on all release (OWASP, 2023).

4. Conclusion

The deployment of these specifications helps ensure that the QRadar DSM API is resilient against typical security threats while facilitating effective data parsing and correlation between interconnected devices. Through considerations of authentication, input validation, and logging, the paper encourages both technological robustness and regulatory adherence (NIST, 2023). Through collaborative efforts, both activities help retain the confidentiality, integrity, and availability of information being processed within the extensive QRadar ecosystem (IBM, 2025).

References

IBM (2025) *IBM QRadar SIEM API Documentation*. Available at: https://www.ibm.com/docs/en/qradar-common?topic=api-endpoint-documentation-supported-versions  
OWASP (2023) *OWASP API Security Top 10 – 2023*. Available at: https://owasp.org/API-Security  
NIST (2023) NIST SP 800-204C: Implementation of DevSecOps for a Microservices-Based Application Using Service Mesh. National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.SP.800-204C>