DeepShield API Documentation v4.0

Effective Date: January 11, 2024

Document Control Number: API-DOC-2024-V4.0

1. Introduction and Scope

1. This API Documentation ("Documentation") is provided by DeepShield Systems, Inc., a Delaware corporation ("DeepShield"), and contains confidential and proprietary information regarding DeepShield's industrial control system (ICS) security platform and related application programming interfaces.

2. This Documentation supersedes and replaces all prior versions of the DeepShield API Documentation, including without limitation versions 3.0 and earlier.

2. Definitions

1. "API" means the DeepShield application programming interfaces described herein.

2. "Authentication Credentials" means the API keys, tokens, certificates, and other security credentials required to access the API.

3. "Client Application" means any software application, system, or service that interfaces with the API.

4. "OT Environment" means the operational technology environment where the API is deployed.

3. API Access and Authentication

1. Access Protocol

- Primary endpoint: https://api.deepshield.com/v4
- Secondary endpoint (failover): https://api-backup.deepshield.com/v4
- Authentication: OAuth 2.0 with JWT tokens
- TLS version requirement: 1.3 or higher

2. Authentication Requirements

- All API requests must include a valid Authentication Token
- Tokens expire after 12 hours

- Rate limiting: 1000 requests per minute per API key
- IP whitelisting required for production access

4. Core API Functions

1. Threat Detection APIs

```
POST /v4/threats/detect
GET /v4/threats/{threatid}
PUT /v4/threats/{threatid}/status
DELETE /v4/threats/{threatid}
```

2. System Monitoring APIs

```
GET /v4/monitor/status
POST /v4/monitor/configure
GET /v4/monitor/metrics
GET /v4/monitor/alerts
```

3. Response Automation APIs

```
POST /v4/response/trigger
GET /v4/response/actions
PUT /v4/response/policies
DELETE /v4/response/rules/{ruleid}
```

5. Security Requirements

1. All Client Applications must:

- Implement end-to-end encryption for all API communications
- Store Authentication Credentials in secure, encrypted storage

- Maintain audit logs of all API access and operations
- Implement automatic session termination after 30 minutes of inactivity

2. Security Protocols

- All requests must use HTTPS with TLS 1.3
- Certificate pinning required for production environments
- Multi-factor authentication required for administrative operations
- Regular security scanning and penetration testing mandatory

6. Data Handling and Privacy

1. Data Classification

- All API data is classified as Confidential
- Personal data handling must comply with GDPR and CCPA
- Data retention limited to 90 days unless otherwise specified
- Secure data disposal required after retention period

2. Data Processing Requirements

- All data must be encrypted at rest and in transit
- Processing limited to authorized geographic regions
- Data anonymization required for analytical purposes
- Regular privacy impact assessments mandatory

7. Compliance and Auditing

1. Compliance Requirements

- SOC 2 Type II compliance mandatory
- ISO 27001 certification required
- NIST Cybersecurity Framework alignment
- Regular compliance audits required

2. Audit Requirements

- Maintain detailed API access logs for 12 months
- Quarterly security assessments

- Annual penetration testing
- Regular compliance reporting

8. Warranty and Liability

1. THE API IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. DEEPSHIELD DISCLAIMS ALL WARRANTIES, INCLUDING BUT NOT LIMITED TO MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

2. IN NO EVENT SHALL DEEPSHIELD BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF THE API.

9. Proprietary Rights

1. All intellectual property rights in the API, including but not limited to patents, copyrights, trademarks, and trade secrets, are owned exclusively by DeepShield.

2. No license or right to use DeepShield's intellectual property is granted except as explicitly provided in a separate license agreement.

10. Version Control

Document Version: 4.0

Last Updated: January 11, 2024

Approved By: Dr. Elena Rodriguez, Chief Security Architect

Document Owner: James Morrison, VP of Engineering