DeepShield API Documentation v2.1

Effective Date: January 11, 2024

Document Control Number: API-DOC-2.1-2024

Classification: CONFIDENTIAL

1. Introduction

This documentation ("Documentation") describes the application programming interfaces ("APIs") and related technical specifications for the DeepShield Industrial Control System Security Platform ("Platform") provided by DeepShield Systems, Inc., a Delaware corporation ("DeepShield"). This Documentation is subject to the Master Services Agreement between DeepShield and its authorized licensees.

2. Definitions

1. "API" means the application programming interfaces described in this Documentation.

2. "API Credentials" means the authentication tokens, keys, and certificates required to access the API.

3. "OT Environment" means the operational technology environment where the Platform is deployed.

4. "SCADA Interface" means the supervisory control and data acquisition system interface components.

5. "Security Event" means any detected anomaly, threat, or security incident within the protected environment.

3. API Architecture

1. **Core Components**

- Deep Layer Security Engine (DLSE) v4.2
- Maritime Operations Module (MOM) v2.3
- Subsea Protection Interface (SPI) v1.8
- Industrial Control System Monitor (ICSM) v3.5

2. **Authentication Protocol**

The API implements OAuth 2.0 with JWT tokens for authentication. All API requests must include a valid Bearer token in the Authorization header.

3. **Endpoint Structure**

Base URL: https://api.deepshield.com/v2.1/

All endpoints use HTTPS with TLS 1.3 or higher.

4. API Methods

1. **Security Event Monitoring**

```
GET /events
POST /events/acknowledge
PUT /events/{eventid}/resolve
```

2. **System Configuration**

```
GET /config
PATCH /config/update
POST /config/validate
```

3. **Threat Detection**

```
GET /threats/active
POST /threats/analyze
PUT /threats/mitigate
```

5. Rate Limits and Quotas

1. **Standard Tier**

- 1000 requests per minute
- 5000 events per hour

- 100 concurrent connections

2. **Enterprise Tier**
- 5000 requests per minute
- 25000 events per hour
- 500 concurrent connections

6. Security Requirements

1. All API communications must be encrypted using TLS 1.3 or higher.

2. API Credentials must be rotated every 90 days.

3. Failed authentication attempts are limited to 5 per minute per IP address.

4. All API access must originate from pre-approved IP ranges.

7. Data Handling

1. **Data Classification**
- Level 1: Public Information
- Level 2: Internal Use Only
- Level 3: Confidential
- Level 4: Highly Confidential

2. **Data Retention**

Security event data is retained for 365 days unless otherwise specified by applicable regulations or contractual requirements.

8. Error Handling

1. **Standard Error Codes**
- 400: Bad Request
- 401: Unauthorized
- 403: Forbidden
- 429: Rate Limit Exceeded
- 500: Internal Server Error

2. **Error Response Format**

```json
{
"error": {
"code": "string",
"message": "string",
"details": "object"
}
}
```

9. Compliance and Certification

1. The API implementation complies with:

- ISO 27001:2013
- IEC 62443
- NIST SP 800-82
- Maritime Cybersecurity Framework (MCF)

10. Legal Notices

1. **Proprietary Rights**

This Documentation and all related intellectual property rights are owned exclusively by DeepShield Systems, Inc.

2. **Confidentiality**

This Documentation contains confidential and proprietary information and may not be disclosed to third parties without DeepShield's prior written consent.

3. **Disclaimer**

DEEPSHIELD PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

11. Version Control

Document Version: 2.1

Last Updated: January 11, 2024

Previous Version: 2.0 (October 15, 2023)

Next Review Date: July 11, 2024

12. Contact Information

Technical Support: api-support@deepshield.com

Security Issues: security@deepshield.com

Documentation Feedback: docs@deepshield.com
