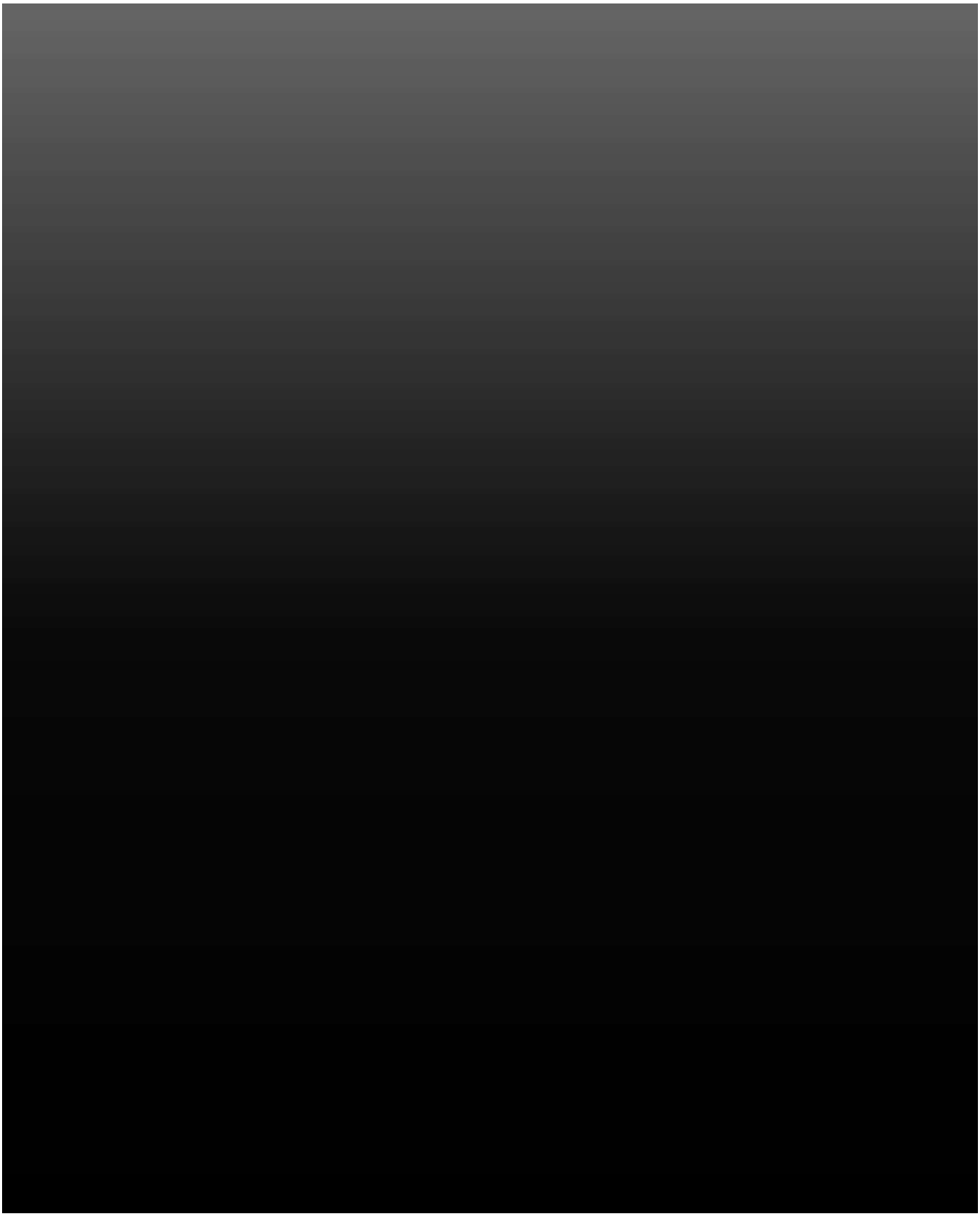
KSADS-COMP Inc.

Application Security

Sep 2026

 www.KSADS-COMP.com v1.3_09_23_26



Contents

KSADS-COMP Process

Securing Applications – At Every Stage

Security should be embedded in every phase of application development to provide protection in its true sense. To accomplish this, we need to understand the complete lifecycle of application development and incorporate security best practices that connects with its individual stages.

Multi-faceted Approach

Any application development starts by gathering the requirement and perform analysis followed by design, code, testing, and deployment into production environment and finally provides ongoing maintenance support. To look at this lifecycle holistically, we need to incorporate security at strategic phases that will help identify gaps and vulnerabilities early on and also provide layered protection.

- Application design and development is where it all begins to materialize and provide shape to an application. It is important to adopt secure coding practice to build a secure application. Static code review will help achieve the objective of identifying and mitigating the vulnerabilities at code level.

- Application Testing phase needs adequate protection to the application. Our dynamic process provides the necessary information that helps the developer to make the security-related modifications while the application is being built.

- Application in production environment is what the world sees. Adding security at this phase is a must as it provides insight to the visibility that the attacker is likely to have.

- Run-time protection is the ongoing mechanism to safeguard the application from external attacks. It is imperative as any leakage of sensitive data leads to financial loss and negatively impacts brand value.

Application Security

KSADS Phase II application (KSADS-COMP) was developed using Microsoft's ASP.NET framework 4.8.1 and a Microsoft SQL Server database 2016 ES3. These technologies have proven to be extremely stable, reliable, and secure. Several aspects of the ASP.NET framework promote reliability and security of the application.

- Code stability and reusability through extensive use of fully tested program libraries (class files)
- Code encapsulation through object-oriented programming. Use of independently tested and verified code objects minimizes system-wide issues
- Separation of programming logic (code-behind classes) from page design for easier identification and resolution of issues
- A separate "Data Access" layer of code responsible for interacting with the database.
- Data is hidden and cannot be accessed by external functions
- The clients' requirement driven business logic is programmed in a separate layer and this architecture helps to scale and maintain the application with less downtime.

The architecture and process used to develop the application are structured to keep the application secured using the following mechanisms: -

Input validation

Input validation is performed to ensure only properly formed data is entering the workflow in an information system, preventing malformed data from persisting in the database and triggering malfunction of various downstream components. Input validations are applied on both syntactical and Semantic level.

Syntactic validation enforces correct syntax of structured fields (e.g., date).

Semantic validation enforces correctness of their values in the specific business context (e.g. start date is before end date, grades are within age limits etc.).

Authentication

Security and privacy have been of the utmost concern in the development of the application. KSADS-comp architecture includes authentication and authorization business logic layers.
The application's authentication process requires the combination of a username and password and on-demand two-factor authentication (2TFA) and to access the content. Data security within the SQL Server database is ensured through two levels of authentication, one at the SQL Server level, and a second at the database level. The application is also designed to defend against security attacks such as SQL injection (e.g., user input is not directly be embedded in SQL statements; rather parameterized statements are used).

Authorization

KSADS-COMP authorization layer is constructed by taking the different user roles into consideration.
User Roles are permission sets that control access to areas and features within the KSADS-COMP environment. KSADS-COMP has super-admin, study-admin, admin, and client user roles for each site. Each user will have specified user roles thus allowing/ denying access to resources and data according to the configured policies. Unauthorized users cannot access features on the site for which they are not authorized to access. They also cannot assess the data from other sites.

Configuration management (CM) is a process for establishing and maintaining consistency of a product's performance, functional and physical attributes with its requirements, design and operational information throughout its life. We are using Atlassian bitbucket for CM.

Session Management is a server-side method of managing the state of an application i.e. all the web applications' state related info are stored on server side. The benefit of having this technique is that since we are keeping all the state related information on server, the request and response becomes lightweight. Also, the chances of someone intercepting or changing this data are also reduced.

Cryptography and Data Encryption

KSADS-COMP does not store user passwords in plain text. Password credentials are protected using cryptographic hashing, and the resulting hash values are used for password verification. When a user enters a password, the application processes the supplied password using the configured hashing mechanism and compares the resulting value with the stored credential value. Plain-text passwords are not stored in the application database. The application uses the bcrypt password hashing algorithm for password storage and verification.

Cryptography is used at a various level since it provides the following benefits: -

- **Confidentiality.** Confidentiality is achieved through encryption, which protects sensitive information from unauthorized access. Encryption algorithms use cryptographic keys to transform readable plain text into an unreadable cipher text. The corresponding decryption process converts the cipher text back into its original form when access is authorized.

Symmetric encryption uses the same cryptographic key for both encryption and decryption, while asymmetric encryption uses a mathematically related public and private key pair. KSADS-COMP applies appropriate encryption mechanisms to protect sensitive data during transmission and, where applicable, while stored.

- **Data integrity.** Data integrity mechanisms protect information from accidental or deliberate unauthorized modification. Cryptographic hashes and Message Authentication Codes (MACs) can be used to detect whether data has been altered.

A cryptographic hash generates a fixed-length value (hash) from a given set of data. When data is received, its hash can be recalculated and compared with the expected hash value to determine whether the data has been modified in transit or during processing. Where authentication is also required, MACs provide integrity verification using a shared secret key.

- **Authentication.** Authentication mechanisms help verify that data originates from a trusted and intended party. Digital certificates are used to establish the identity of parties and support secure communications. Digital signatures provide a mechanism for verifying both the authenticity and integrity of digitally signed data. In practice, digital signatures are typically generated over a cryptographic hash of the original data, which provides an efficient way to sign and subsequently verify the data.

Parameter Manipulation

Query-string parameters are used only where necessary. All input parameters received through form fields, query strings, and HTTP headers are subject to server-side validation to help prevent unauthorized or malicious parameter manipulation.

Session state is used where server-side state management is required rather than relying on client-side View State.

The application does not use application-managed cookies for storing user data or application state.

Exception Management

The application implements structured exception handling to manage unexpected errors and application exceptions in a controlled manner. Exceptions are handled using the .NET/Microsoft exception-handling framework, with appropriate error handling and logging mechanisms to support troubleshooting and security monitoring.

Detailed technical exception information is not exposed to end users. Instead, users are presented with appropriate, user-friendly error messages while sensitive implementation details, such as stack traces and internal system information, are protected from disclosure.

Transport Layer Security (TLS)

KSADS-COMP uses **Transport Layer Security (TLS) 1.2** to protect data transmitted between users and the application. TLS provides encryption for data in transit, helping prevent

unauthorized parties from intercepting or accessing sensitive information while it is being transmitted over the network.

TLS also provides server authentication through digital certificates issued by trusted Certificate Authorities (CAs). This helps users establish that they are communicating with the intended application server and helps protect against man-in-the-middle attacks.

The application is configured to use HTTPS for secure communications using TLS 1.2. Appropriate server and certificate configurations are maintained to support secure encrypted communication.

TLS protects the confidentiality and integrity of information transmitted between the client and server; however, it does not by itself protect against phishing emails or fraudulent websites. Users should therefore access the application through the organization's official URL and follow established security practices.

Network Firewall and Security Controls

A KSADS-COMP is hosted within the AWS cloud environment and is protected using network-level security controls designed to restrict unauthorized network access. AWS security controls, including **Security Groups and Network Access Control Lists (NACLs),** are used to control inbound and outbound network traffic based on defined rules and permitted ports and protocols.
These controls help reduce the application's exposure to unauthorized network access and mitigate common network-based threats, including:

- Unauthorized access and network reconnaissance
- Denial-of-service and other network-based attacks
- Exploitation of exposed or unauthorized network services
- Protocol-based attacks targeting network services
- Unauthorized access to application infrastructure
- Network-level interception or eavesdropping

In addition to network controls, application-level security mechanisms are implemented to address threats such as unauthorized access, credential attacks, and malicious input. AWS infrastructure and application security controls are maintained in accordance with the application's security requirements and operational procedures.

Server Security

The KSADS-COMP is hosted within the **Amazon Web Services (AWS) cloud environment**. AWS provides a comprehensive security infrastructure designed to support organizations with stringent security and compliance requirements. Security is implemented through a combination of AWS infrastructure controls and application-level security measures.
Relevant AWS security capabilities include:

- **Infrastructure Security** – Physical and infrastructure-level protections provided by AWS data centers and cloud infrastructure.
- **Network Security and DDoS Protection** – Network access controls and AWS security

mechanisms help protect resources against unauthorized network access and denial-of-service attacks.

- **Data Encryption** – Encryption mechanisms are used to protect sensitive data during transmission and, where configured, while stored.
- **Configuration and Asset Management** – AWS provides capabilities for managing and monitoring cloud resources and their configurations.
- **Monitoring and Logging** – AWS monitoring and logging services can be used to monitor infrastructure activity, security events, and operational activity.
- **Identity and Access Management** – Access to AWS resources is controlled through authentication, authorization, and role-based access mechanisms.
- **Security Testing** – AWS permits security testing of customer-controlled cloud resources in accordance with its security testing policies and requirements.

Infrastructure Security

AWS provides a range of infrastructure and network security capabilities that can be used to protect cloud-hosted applications and control network access. For KSADS-COMP, applicable infrastructure security controls include:

- **Network Access Controls:** Amazon Virtual Private Cloud (VPC) provides network isolation and enables control of inbound and outbound traffic through security controls such as **Security Groups** and, where configured, **Network Access Control Lists (NACLs)**.
- **Web Application Protection:** AWS provides **AWS WAF** capabilities for protecting web applications against common web-based attacks. Where enabled and configured for the application, WAF rules can be used to inspect and control HTTP/HTTPS requests.
- **Encryption in Transit:** Communications between users and the KSADS-COMP application are protected using **HTTPS with TLS 1.2**, helping maintain the confidentiality and integrity of data during transmission.
- **Private Connectivity:** AWS provides options for private and dedicated connectivity between cloud resources and on-premises environments where required.
- **AWS Network Infrastructure:** AWS maintains security controls across its global cloud infrastructure and network. Protection and encryption of traffic between AWS services and facilities depend on the specific AWS services, configuration, and communication path being used.

Cloud Computing

KSADS-COMP is hosted in the **Amazon Web Services (AWS) cloud environment**. Cloud computing provides on-demand access to computing resources and services, including servers, storage, databases, networking, and other application services over the Internet.
AWS operates and maintains the underlying cloud infrastructure, including the physical data centers, networking equipment, and hardware required to deliver these services. This allows KSADS-COMP to leverage AWS's infrastructure and security capabilities while maintaining appropriate application-level security and access controls.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) provides an additional layer of security beyond a username and password. When enabled, users are required to provide an additional authentication factor, such as a verification code generated by an authenticator device or application, in addition to their primary credentials.
AWS Identity and Access Management (IAM) supports MFA to help protect access to AWS accounts and resources. MFA can be applied to privileged and administrative accounts to reduce the risk of unauthorized access in the event that primary credentials are compromised. Access to AWS resources is controlled through appropriate authentication and authorization mechanisms, with MFA applied in accordance with the organization's security and access-control requirements.

IP Whitelisting

Administrative access to the KSADS-COMP hosting environment is restricted to authorized personnel. Where applicable, network-level access controls are configured to permit administrative connections only from approved IP addresses or trusted network locations. Access is further protected through authentication and authorization controls, and administrative privileges are limited to authorized personnel based on their assigned roles and responsibilities.

Compliance

The AWS cloud infrastructure used to host KSADS-COMP is supported by a comprehensive portfolio of security certifications, attestations, and compliance programs. These demonstrate that AWS maintains security and operational controls aligned with various internationally recognized standards and regulatory requirements.

Relevant AWS compliance programs and certifications include, as applicable:

- **SOC 1, SOC 2, and SOC 3**
- **ISO/IEC 27001** – Information Security Management
- **ISO/IEC 27017** – Cloud Security

- **ISO/IEC 27018** – Protection of Personally Identifiable Information in Public Clouds
- **PCI DSS** – Payment Card Industry Data Security Standard
- **FedRAMP** – Federal Risk and Authorization Management Program
- Other applicable industry and regulatory compliance programs supported by AWS.

Penetration-Testing for GDPR

KSADS-COMP has undergone a **third-party penetration test** to assess the security of the web application and its supporting infrastructure. The assessment was conducted by **DongIT** and was intended to identify security vulnerabilities and potential weaknesses that could be exploited by an attacker.

The assessment methodology was informed by established industry security practices and recognized security frameworks, including:

- **Open Worldwide Application Security Project (OWASP)**
- **Information Systems Security Assessment Framework (ISSAF)**
- **Open-Source Security Testing Methodology Manual (OSSTMM)**
- **Penetration Testing Execution Standard (PTES)**
- **National Institute of Standards and Technology (NIST)** security guidance

The assessment covered relevant areas of the KSADS-COMP environment, including web application security and applicable infrastructure and network security controls. Testing included checks for common vulnerabilities such as **SQL injection, Cross-Site Scripting (XSS), authentication and authorization weaknesses, brute-force attacks, input validation issues, and other security vulnerabilities**.

Findings identified during the assessment were reviewed and addressed through the application's security remediation process. Appropriate corrective actions were implemented based on the findings and their associated risk.

Penetration testing forms part of the broader security assessment and risk-management process and supports the ongoing identification and remediation of potential security weaknesses.

Benefits of Penetration Testing

Penetration testing supports the organization's overall security and risk-management program by helping to:

- **Identify and prioritize security risks** based on the vulnerabilities identified during the assessment.
- **Reduce the risk of unauthorized access** by identifying weaknesses that could potentially be exploited by attackers.
- **Strengthen the organization's security posture** by providing actionable findings for security improvements.
- **Reduce the potential impact of security incidents** by identifying and addressing vulnerabilities before they can be exploited.
- **Support applicable security and regulatory requirements** by providing evidence of security assessment and vulnerability-management activities.

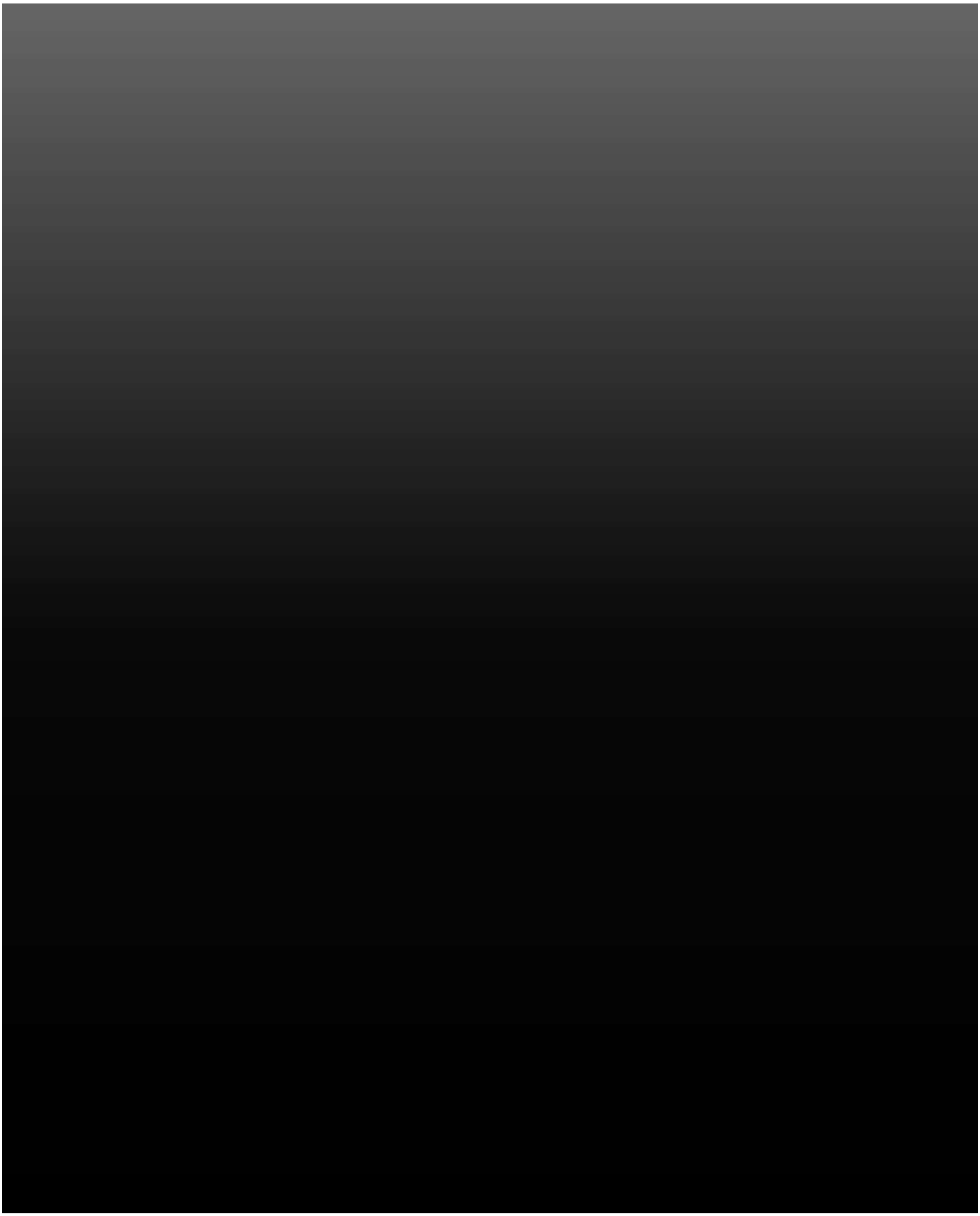
For more information on the other AWS Security Platform security measures please visit this link: https://aws.amazon.com/security/

Key Contacts

Joan Kaufman, PhD
KSADS-COMP co-developer

Kenneth Kobak, PhD
KSADS-COMP co-developer

Alison Deep, MCA
KSADS-COMP IT director



KSADS-COMP Inc.

The gold standard in child and adolescent psychiatric diagnoses.

 www.KSADS-COMP.com v1.3_09_23_26