AppOmni

DATASHEET

SaaS Event Maturity Matrix (EMM)

Gain clarity & enhance SaaS security with insights into SaaS logs

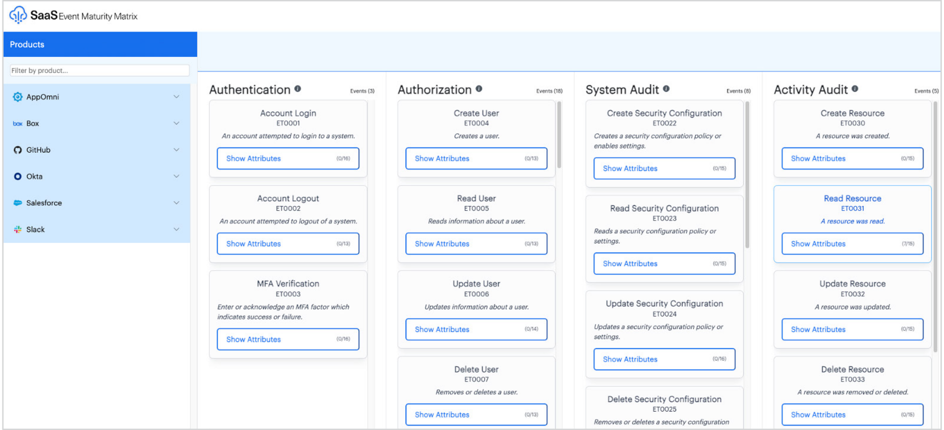
SaaS Monitoring Challenges

Software as a Service (SaaS) is now the backbone of business operations, offering unparalleled flexibility, scalability, and integration. But this growth has made SaaS platforms more vulnerable to data breaches and suspicious activities, and it's now crucial that security teams can monitor these platforms continuously for potential security issues.

Despite the clear need for SaaS monitoring, there is a lack of consistency in SaaS events and audit logs, which makes it difficult to monitor for cyber threats. Log formats vary from one application to another and are inconsistent across data structure, context, and metadata. This lack of unity and consistency complicates security because it leaves gaps in threat detection and requires that teams waste valuable time evaluating applications.

Event Maturity Matrix (EMM)

The Event Maturity Matrix (EMM) is an open-source framework, developed by AppOmni, that highlights visibility gaps and boosts the efficiency of cybersecurity teams. The EMM helps you evaluate and refine the audit logging functions of your SaaS platforms so that you can enhance threat detection and response actions in your organization.



Authentication — Events (3)

Account Login
ET0001
An account attempted to login to a system.
Show Attributes (0/16)

Account Logout
ET0002
An account attempted to logout of a system.
Show Attributes (0/13)

MFA Verification
ET0003
Enter or acknowledge an MFA factor which indicates success or failure.
Show Attributes (0/16)

Authorization — Events (18)

Create User
ET0004
Creates a user.
Show Attributes (0/13)

Read User
ET0005
Reads information about a user.
Show Attributes (0/13)

Update User
ET0006
Updates information about a user.
Show Attributes (0/14)

Delete User
ET0007
Removes or deletes a user.
Show Attributes (0/13)

System Audit — Events (8)

Create Security Configuration
ET0022
Creates a security configuration policy or enables settings.
Show Attributes (0/15)

Read Security Configuration
ET0023
Reads a security configuration policy or settings.
Show Attributes (0/15)

Update Security Configuration
ET0024
Updates a security configuration policy or settings.
Show Attributes (0/16)

Delete Security Configuration
ET0025
Removes or deletes a security configuration

Activity Audit — Events (5)

Create Resource
ET0030
A resource was created.
Show Attributes (0/15)

Read Resource
ET0031
A resource was read.
Show Attributes (7/15)

Update Resource
ET0032
A resource was updated.
Show Attributes (0/15)

Delete Resource
ET0033
A resource was removed or deleted.
Show Attributes (0/15)

AUDIT LOG CHALLENGES

- SaaS apps have different methods for authentication, data retrieval, and other activities
- SaaS logs lack standard schema and use different parameters
- Normalizing and searching SaaS logs is time-intensive

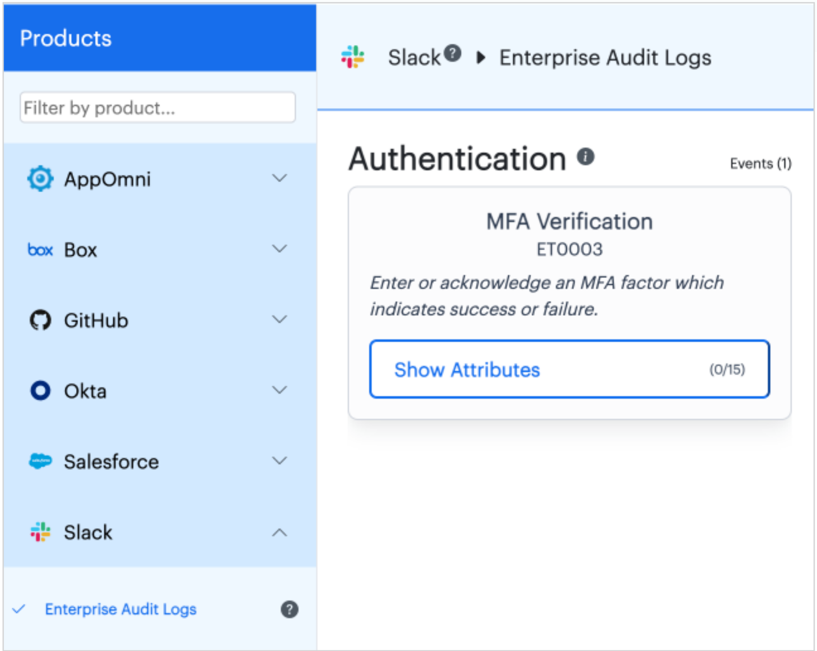
EVENT MATURITY MATRIX BENEFITS

- **Unify documentation:** Centralize necessary documentation for better accessibility and understanding
- **Identify gaps:** Clearly map audit log sources to facilitate log detection and analysis
- **Improve investigations:** Understand what data is provided in logs to engineer detections and plan for

Using the Event Maturity Matrix

Conduct vendor assessments

- Determine what log data is provided from a SaaS application
- Verify data that is needed for continuous monitoring and SaaS visibility

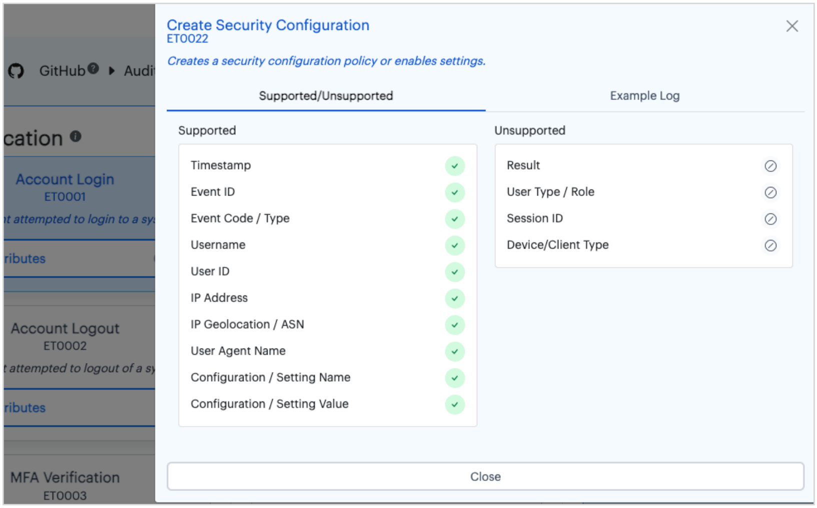


MFA Verification
ET0003
Enter or acknowledge an MFA factor which indicates success or failure.

Slack does not have logs to identify MFA

IR and detection research

- Quickly determine audited actions and field that are available during a SaaS incident
- Find example events for building threat detection rules



Create Security Configuration
ET0022
Creates a security configuration policy or enables settings.

Supported		Unsupported	
Timestamp	✓	Result	⊘
Event ID	✓	User Type / Role	⊘
Event Code / Type	✓	Session ID	⊘
Username	✓	Device/Client Type	⊘
User ID	✓		
IP Address	✓		
IP Geolocation / ASN	✓		
User Agent Name	✓		
Configuration / Setting Name	✓		
Configuration / Setting Value	✓		

Github list of unsupported fields for "Create Security Configuration"

Check out the matrix on GitHub or the EMM website.

What users are saying:

> This will provide our security team continuous monitoring of security events for all new SaaS and I'm also going to leverage this approach to get visibility into our top 50, then top 100 apps.
>
> **— Fortune 100 SOC director**

> [We've] included EMM in our vendor due diligence process to provide our security team with actual value from the effort beyond the initial point in time assessment... I send it to new vendors as a requirement to fill out in order to be approved and to existing vendors during their annual security reviews.
>
> **— Security architect at a top three telecommunications vendor**