APPSIAN

SOLUTION BRIEF

Application Security Platform
Real-Time Analytics

Abstract

Your ERP applications house your organization's most sensitive data, making them a tempting target for cyber-attacks. The increasing frequency of cyber-attacks on ERP systems calls for improved threat detection and remediation features in your security infrastructure. In July 2018, the Department of Homeland Security issued a warning outlining an increased number of threats against ERP systems. The warning was based on intelligence that uncovered a 160% surge in interest and activity around ERP-specific vulnerabilities.

In addition, regulatory bodies around the globe are establishing strict data privacy mandates concerning the storage, usage, and sharing of personally identifiable information (PII). Data protection regulations have also enforced stringent timelines for the reporting and remediation of breaches. Non-compliance with these regulations will not only result in extensive monetary penalties, but also can cause irreparable damages to an organization's existing clientele, new business opportunities and brand reputation.

To prevent ERP data breaches originating from phishing, brute force attacks, data leaks, privilege abuse and more, organizations need real-time visibility into how, when, and by whom their ERP systems are being accessed. *But, how do organizations investigate thousands of user transactions and determine what needs immediate attention?* The solution lies in data visualization. Taking all user transaction data and aggregating it into visually compelling dashboards that highlight patterns, trends, and anomalies can help security personnel detect and respond to threats quickly.

Featured Highlights

Challenges

To safeguard ERP systems against security threats, intrusions, and data loss, organizations need a robust analytical tool to monitor how sensitive data is accessed. The lack of detailed user activity logs in legacy ERP applications (for example: PeopleSoft and SAP) prevents organizations from having a clear view of how, when, and by whom specific data fields were viewed. Given the ubiquitous nature of outsider intrusions, along with the prevalence of insider threats, security professionals must have a "transaction level" view of activity in order to spot trends that could be indicative of malicious activity.

Solution

Appsian's Real-Time Analytics integrates seamlessly into your ERP environment to provide unparalleled detection and response capabilities. Leveraging advanced visual dashboards, security professionals are given a high-level (and granular) view of user activity – displaying the essential trends necessary to identify and mitigate issues that could signify a data breach.

- Analyze access trends based on individual IPs viewing sensitive data
- Trend activity by user and data attributes (sensitivity, privilege, geography etc.)
- View failed login or multifactor authentication attempts
- Detect brute force attacks and suspicious login activity
- Accelerate incident response with quick detection and user-level drill down

Challenges

Data breaches in ERP systems are typically inconspicuous

Data breaches don't summon law enforcement like a home security system does when someone breaks in. Using phishing and spear phishing attacks, cyber criminals obtain valid credentials from your users and then leverage them to breach ERP applications. These hackers can continue to exist inside the system - siphoning data, financials and other critical business information for months or even years before getting noticed. According to a 2017 Ponemon Institute data breach survey, *"hackers spend 200 days in an enterprise system on average before getting detected"* [2], costing organizations approximately $8 million dollars per threat [3]. While cyber criminals have ample time to formulate their strategy, security teams need to be quick in remediating threats to prevent data loss and maintain system integrity. The ability to spot breaches instantly can save enterprises from incurring monetary and reputational damages caused by loss of important data.

Insider data leakage (intentional and unintentional) make up the majority of breaches

Due to the high volume of PII across applications, ERP systems are susceptible to a variety of insider threats that can cause severe breaches from both malicious and unintentional activity. A report [4] from the Ponemon Institute *insider threats are the cause of 60% data breaches and are more difficult to detect and manage than external threats.*

Insider threats are particularly challenging to handle as it is difficult to distinguish whether users are accessing sensitive information for legitimate reasons or with malicious intent. A lack of logging features that provide visibility into user activity and the challenge of implementing effective access controls makes ERP applications vulnerable to threats from internal high privilege users, or even third parties such as contractors, vendors, etc.

For example, in PeopleSoft, user activity logging is capable (out-of-the-box) of only high-level credential activity; where the system only records instances when users log in and out. These instances do not differentiate between a genuine login or credential misuse and offer little insight into how users are interacting with the information on various pages. Given that the majority of modern security threats are executed with valid login credentials, deeper visibility into transaction level activities is necessary to prevent or minimize data breaches.

Compliance requirements are escalating (and have become time sensitive)

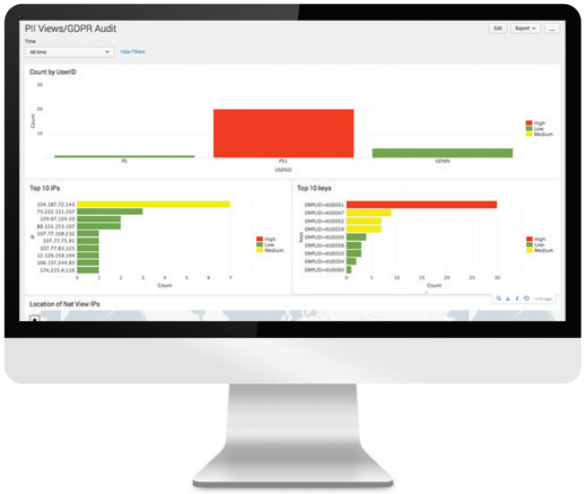
Regulatory bodies like the US Department of Education, the European Union, the State of California and more have introduced data privacy mandates requiring organizations to notify affected individuals of PII breaches in a stipulated amount of time. For example – under the General Data Protection Regulation (GDPR), the European Union will levy fines up to 4% of global annual revenue or €20 Million (whichever greater) if organizations fail to notify the appropriate supervisory authority within 72-hours of identifying a breach. More regulatory bodies are likely to follow with similar directives in the near future, and non-compliance with these regulations is set to cost organizations millions of dollars.

Before sending a breach notification, organizations need to fully understand a breach and have remediation activities well underway. However, traditional security audits performed manually on excel sheets are time consuming – taking weeks or even months. Moreover, the limited information acquired from native logs is inadequate for timely detection of breaches and subsequent remediation efforts. To comply with these time-sensitive breach notifications, organizations need real-time visibility into transactions in order to detect suspicious activity, identify vulnerabilities, prevent breaches, and minimize negative impacts.

Solution

Accelerate threat detection, reporting, and response

Appsian's Application Security Platform features an insight extension called Real-Time Analytics. As the Application Security Platform's logging feature records all user activity for all transactions, data trends are aggregated and visualized using engaging and visually rich dashboards.



This enhanced data visibility equips security professionals with the insight they need to get ahead of security threats and detect vulnerabilities posed not only by network intrusions, brute-force attacks, and phishing, but also insider threats like privilege abuse, data mishandling, and more.

Strengthen your audit response strategies for improved compliance

GDPR requires organizations to report data breaches within 72 hours or face severe non-compliance penalties. The time required to identify and react to a data breach has become a significant factor in staying compliant with GDPR.

Using **Real-Time Analytics,** ERP activity can be visualized by various parameters such as activity patterns, user groups, locations and more. Thus, enabling organizations to identify breaches in real-time and quickly pursue remediation activities. By fast-tracking this process, organizations are empowered to stay compliant with internal governance policies along with external regulations.

How does it work?

Application Security Platform allows **Real-Time Analytics** to be plugged directly into the ERP web server, without requiring any additional hardware. After leveraging transaction logs (supplied by ASP), data is then populated and displayed in **Splunk-leveraged dashboards.** Comprising of elegant charts, graphs and maps, these dashboards can be grouped by usage patterns, access trends, geographical locations, and more to gain a holistic picture of user activity in a single view. The dashboards are equipped with deep drill down capabilities, allowing security teams to thoroughly investigate activity and perform root cause analysis.

Security Insights

Intrusion Prevention

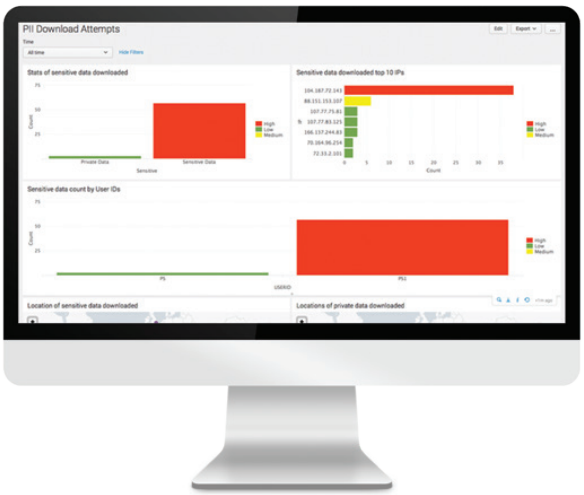
- Brute Force Attack detection
- Authentication attempt trends
- Geographical location of an access

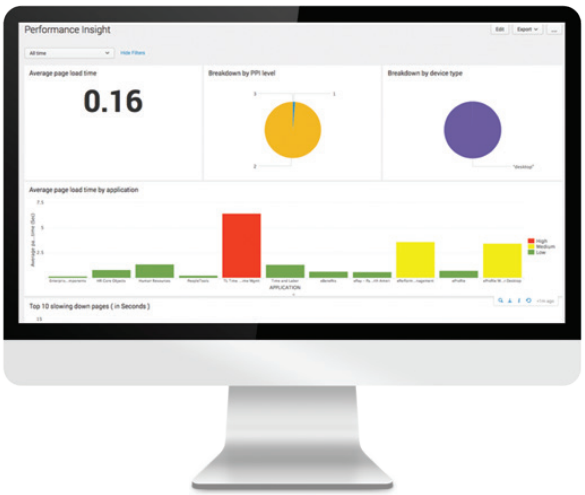
Data Loss Protection

- Security Changes
- Trending data access by sensitivity
- Trending privileged user access

Incident Response

- Detecting attacks/breaches
- Forensics at user / IP level





References

[1] https://www.us-cert.gov/ncas/current-activity/2018/07/25/Malicious-Cyber-Activity-Targeting-ERP-Applications

[2] https://www-01.ibm.com/marketing/iwm/dre/signup?source=urx-15763&S_PKG=ov58441

[3] https://www.itgovernanceusa.com/blog/how-long-does-it-take-to-detect-a-cyber-attack/

[4] https://www.observeit.com/ponemon-report-cost-of-insider-threats/

APPSIAN

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

(469) 906-2100

info@appsian.com