Applied AI
Intelligence Delivered

aws partner network
Advanced Consulting Partner

Information Security Management System ISO 27001 Certified

CASE STUDY

Ensured Optimum Security by Scanning **Log4j Vulnerabilities** with AWS Inspector

EXECUTIVE SUMMARY

The client - A logistics platform company. They offer easy-to-use apps to help contractors, dump-truck owners, and material producers to provide exceptional services with full visibility and more efficiently. Their logistic platform simplifies retail and supply chain across the globe.

In this case study, we will explain how AAIC helped the customer in overcoming the Log4j threat within a short span of time.

THE CHALLENGE

- We have been supporting the client with DevOps services to transform their software delivery pipeline.
- The client's app was using Log4J - the java library. As soon as the Log4j threat was detected and declared as the worst vulnerability in 10 years by Apache, the client got scared, and contacted our dedicated AWS security team.
- As the leading AWS partner, we help address and solve all cloud and security issues.
- We deployed our **AWS security experts** to resolve the issues asap.

The key issues we found were:

OUR SOLUTIONS

We provided the following solutions to mitigate the Log4j threats:

Setup AWS WAF correctly

The first thing we did was checking the WAF and setting up two rules, i.e. AWS Managed Rules (AMR). These rules offer protection against malicious activities.

We set **AWSManagedRulesKnownBadInputsRuleSet** to inspect the request body, and commonly used headers.

We set **AWSManagedRulesAnonymousIpList** to block requests from services that allow the confusion of viewer identity.

AWS SECURITY EXPERT ACTIONS

01.
We ran an assessment with AWS Inspector to scan the Log4j library

02.
The assessment included 60 instances, and was tested against 2 Rules Packages

03.
We checked:
- Common Vulnerabilities and Exposures
- Security Best Practices

04.
Checked whether the EC2 instances in the client's app are exposed to Common Vulnerabilities and Exposures (CVEs)

05.
Checked whether the client's systems are configured securely

06.
Checked 60 instances along with vulnerability of the images

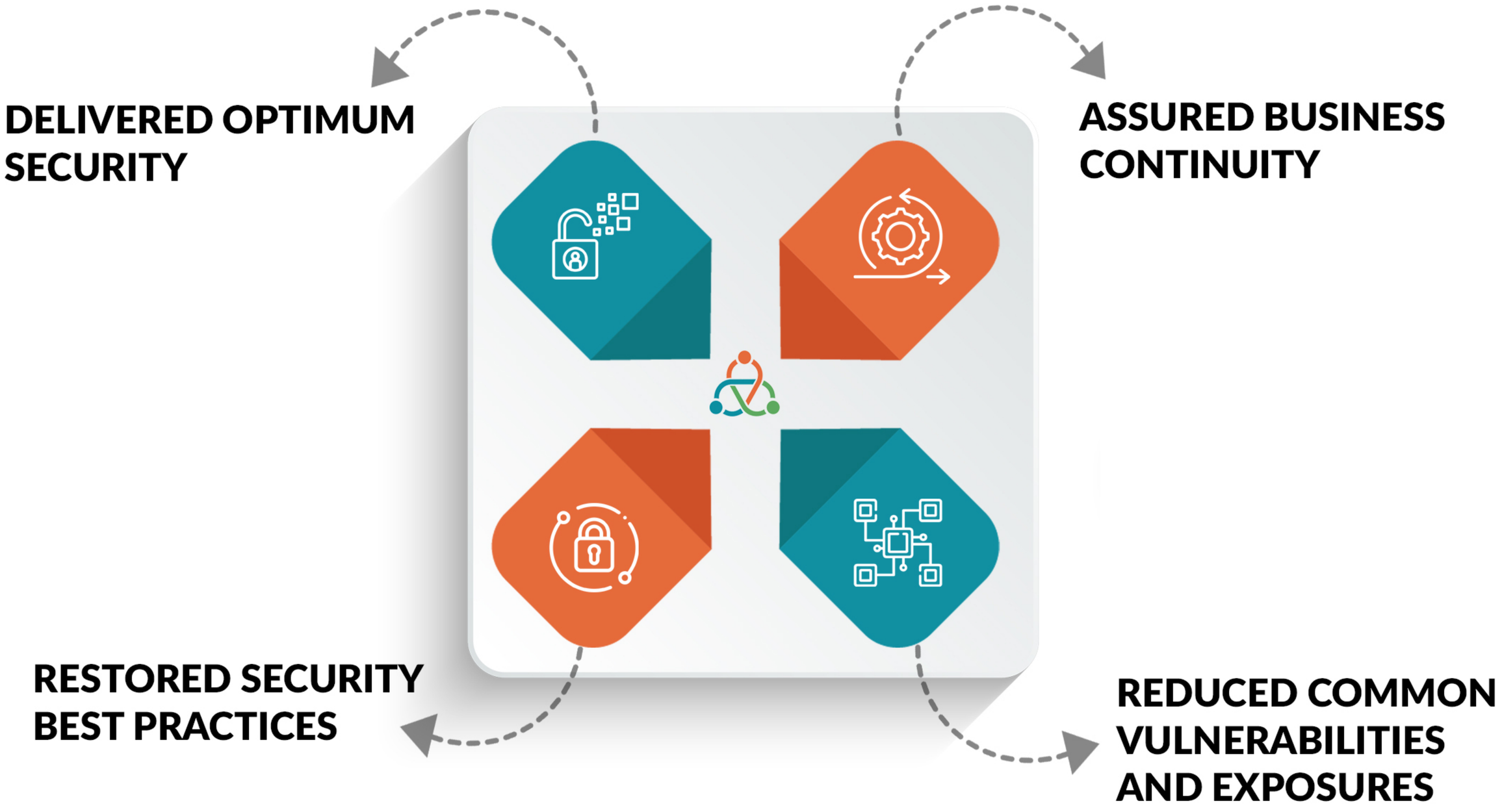
LOG4J UPGRADE

The version of our client's Log4j library was 2.14.1 that was vulnerable.
Hence, our team of AWS security experts upgraded it to the latest and safe version.

ECR - PATCH CONTAINER IMAGES

We scanned the ECR which is a AWS managed container image registry service. Our team found 10 vulnerabilities in the client's repository. Hence, we upgraded the images with the right versions and pushed them to the repository. The AWS inspector checked and verified them for any threat possibility.

RESULTS AND BENEFITS



ABOUT AAIC

We are automation experts, with a majority(> 60%) of our workforce AWS-certified.
We assist you in applying intelligence to the Cloud and DevOps, as our name suggests.

Our AWS certified experts create high-performing cloud apps by utilizing intelligent components and smart integrations to accelerate your digital transformation journey.

+91-9923354746
connect@appliedaiconsulting.com
www.appliedaiconsulting.com

DevOps
In-a-box
Fastrack your DevOps implementation

Applied AI
Intelligence Delivered