TEVORA™

Case Study

Tevora's Robust Security Assessment Empowers Global Software Company in Evaluating Acquisition Targets

If your company is routinely involved in acquisitions, you probably know how important and challenging it is to assess the security of each acquisition target. Security assessments are a key factor in determining:

- How secure the target firm's environment is currently
- How much work will be needed to align the acquisition target with your security requirements
- How much you are willing to pay to acquire the target firm

In addition, assessments must often be completed on a tight timeline.

With so much riding on the quality and timeliness of acquisition security assessments, it's not surprising that many companies turn to third-party experts like Tevora for help.

In this case study, we'll explain how a leading global software company uses Tevora's experienced team to perform security assessments for its steady stream of acquisitions each year. To protect our client's confidentiality, we'll refer to them by the fictitious name of Global Software Solutions (GSS).

Tevora Engaged

Over three years ago, GSS made a strategic decision to accelerate growth by ramping up its acquisitions to roughly 15-20 per year. As part of this acceleration, they evaluated several leading security consulting firms as potential partners to improve the quality and thoroughness of their acquisition security assessments and enable them to perform more assessments each year.

After completing their evaluation, GSS selected Tevora as their strategic acquisition security assessment partner.

Project Initiation

We held a kickoff meeting to meet key staff members and learn about GSS's objectives, business operations, and overall security and technical environment. We also asked for guidance on the scope and types of due diligence criteria they wanted Tevora to use for conducting acquisition security assessments.

After discussing alternatives for conducting assessments, we settled on a two-pronged approach involving:

1	2
Penetration Testing	**Cloud Technical Due Diligence**
focused on identifying vulnerabilities in the acquisition target's applications.	focused on identifying vulnerabilities in the target company's cloud environment.

Customized Assessment Methodologies

Having agreed on the two-pronged assessment approach, we reviewed our penetration testing and cloud technical due diligence methodologies with the GSS team and customized them to align and integrate with the overall GSS acquisition process.

Tevora Begins Performing Assessments

As GSS began executing its strategic plan to ramp up acquisitions, Tevora's team swung into action, performing security assessments for all new acquisitions. In the first year, we made some minor refinements to our penetration testing and cloud technical due diligence methodologies as we learned more about the GSS acquisition process based on real-world experience performing 16 assessments.

By the end of the first year, we had developed strong working relationships with the GSS acquisition and security teams. We also earned the trust and respect of GSS executives based on the substantial improvements we had made in the quality, thoroughness, timeliness, and quantity of GSS's acquisition security assessments.

Tevora's Penetration Testing Methodology

Our elite threat team combines years of industry experience with exceptional outside-the-box thinking and industry certifications to deliver state-of-the-art penetration testing. We go beyond simple automated tools testing to help GSS understand whether the target firm's current controls and technologies effectively protect its web applications, thick clients, and APIs from external and internal threats.

Here's a summary of the penetration testing methodology we use in support of GSS's acquisition process:

1. Kickoff Meeting with Acquisition Target Firm
   - Review of Tevora penetration testing methodology and timing.
   - Walkthrough of systems environment, web applications, thick clients, and APIs.
2. Reconnaissance
   - Whitebox testing.
   - Enumeration of URLs and endpoints.
   - Open-source intelligence gathering.
   - Client-side application analysis.
3. Assessment
   - Identification of vulnerabilities.
   - Testing input validation.
   - Use of latest OWASP testing guidelines.
   - Application logic testing.
   - Authentication, authorization, and session management testing.
4. Reporting
   - Executive summary for management.
   - Detailed findings report with remediation recommendations.
   - Retesting with validation.
   - Executive presentation.
   - Third-party reporting.

Tevora's Cloud Technical Due Diligence Methodology

Tevora's team of security experts conducts an in-depth review of the target firm's AWS, Azure, or GCP cloud environments using the Tevora Cloud Security Framework. This proprietary assessment methodology draws on Amazon WAR, Azure, and GCP guidelines as well as industry best practices.

As part of our review, we benchmark the target firm's cloud workload against industry best practices to determine if their environment is secure. We also assess whether they have adequate capacity to support the required post-acquisition security and workload requirements.

Our experts partner with the acquisition target firm to identify vulnerabilities in their cloud environment and areas that are not compliant with applicable security standards. We also provide recommendations for improving the target firm's security and compliance posture, managing its cloud environments, and positioning its cloud architecture to integrate with GSS's environment.

Here's a summary of the cloud technical due diligence methodology we use in support GSS's acquisition process:

1. Kickoff Meeting with Acquisition Target Firm
   - Review of Tevora cloud technical due diligence methodology and timing.
   - Manual review of target firm's technical architecture and environment.
2. Cloud Security Review
   - Manual review of security architecture, tools, controls, and environments, including public and private subnets.
   - Identification of applications.
   - Identification of hardcoded secrets and other vulnerabilities.
   - Identification of trust boundaries.
   - Development or updating of cloud architecture diagrams.
3. Threat Modeling
   - Identification of assets, actors, entry points, components, use cases, trust levels, data stores, logs, and encryption.
   - Design diagram development.
   - Identification of threats, attack vectors, and likely attack scenarios.
   - For each threat, identification of mitigations, including any control implementations.
   - Development and review of risk matrix indicating whether each threat is adequately mitigated.

4. Data Flow Documentation
   - Documentation and diagraming of data environments and data flows.
   - Includes data sources, data stores, and how data is used by internal and external organizations.
5. Reporting
   - Executive summary for management.
   - Detailed findings report with remediation recommendations.
   - Retesting with validation.
   - Executive presentation.
   - Third-party reporting.

Benefits

GSS has realized significant benefits as a result of their acquisition security assessment partnership with Tevora, including:

- Average time required to complete penetration testing reduced from 6 weeks to 3.5 weeks.
- Average time required to complete cloud technical due diligence reduced from 8 weeks to 5.5 weeks.
- GSS capacity to perform acquisition security assessments increased from 4 to 20 assessments per year.
- Quality and thoroughness of acquisition security assessments increased significantly.
- Substantially fewer post-acquisition "surprise" discoveries of security vulnerabilities.
- Vast majority of Tevora assessments have been completed on or ahead of schedule.

Commonly Identified Vulnerabilities

In the time we've been performing acquisition security assessments for GSS, here are some of the most common vulnerabilities we've identified:

- Publicly-facing resources that should not be accessible by the public.
- Hardcoded credentials.
- Databases that are not hardened.
- Overly broad access privileges (access not restricted by individual roles).
- Use of default or weak passwords.

Positive Feedback from GSS

We've been partnering with GSS for over three years and have received highly positive feedback from GSS's management and acquisition teams on our performance. They have been particularly pleased with our ability to understand and document extremely complex environments and dig deep to uncover vulnerabilities that other security consultants might have missed.

And perhaps the strongest endorsement is that GSS remains a valued customer for Tevora, and we continue to perform 15-20 acquisition security assessments per year for them.

Let Tevora be Your Trusted Partner

If you'd like to learn more about Tevora's acquisition security assessment services, or engage us to help with your acquisitions, just give us a call at (833) 292-1609 or email us at sales@tevora.com.