Customer Success Story

The Company

This organization is an IT security consulting specialist focused on helping private companies and government agencies protect their computing assets and sensitive information from external attacks and subsequent data breaches. Founded in 2001 and based in the Midwest, the consultancy specifically aims to assist organizations in the identification and assessment of their most significant areas of IT security risk -- and with the process of applying technological and policy-based controls to address problematic areas.

The founder and chief technology officer (CTO) of the organization brings 15-plus years of experience as a military analyst, consultant and chief security officer to bear on the most pressing IT systems defense and compliance management issues faced by his customers. Using products including CORE Impact Pro, the CTO helps those organizations establish comprehensive, sustainable vulnerability assessment and management programs.

Solution Summary

<table>
<thead>
<tr>
<th>CUSTOMER TYPE</th>
<th>Security consultancy</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHALLENGE</td>
<td>Helping customers create and implement effective, repeatable vulnerability management programs to use on an ongoing basis.</td>
</tr>
<tr>
<td>SOLUTION</td>
<td>CORE Impact® Pro, the first comprehensive penetration testing software solution for assessing organizations’ most significant IT vulnerabilities and information security threats.</td>
</tr>
</tbody>
</table>

“We consistently find big gaps between customer expectations and realities when it comes to how well their security controls are functioning. What you don’t know can, in fact, hurt you – and you don’t know what you’re missing until you test your safeguards.”

The Challenge

The organization’s goal is to not only advise its vulnerability assessment services customers on where their biggest weaknesses lie, but also allow them to establish a repeatable testing program that fosters more consistent security on a day-to-day basis.

By creating a sustainable, long-term process for gauging network, application and end-user security vulnerabilities, the company promises its customers the ability to continually self-diagnose risks and “operationalize” their assessment capabilities to better secure data and remain compliant with government and industry regulations.

“Most security teams are buried from an operational perspective and too busy putting out day-to-day fires to get a forward-looking view into what their most significant IT security risks may be,” said the CTO. “We want to help customers move from this reactionary mode into more proactive security, allowing them to work smarter with repeatable processes that help them get ahead of threats and compliance requirements.”

By creating the ability for organizations to measure, prioritize and address IT security risks on a regular schedule, those customers will be able to avoid painful data breaches and prove their due diligence in protecting information when compliance auditors come knocking.

The Solution

To help customers build a framework for vulnerability assessment and management, the CTO encourages organizations to invest in a handful of products that they can apply to their networks, applications and employees on a regular basis to maintain a comprehensive understanding of where their defenses stand at any given moment in time.

Along with vulnerability scanning tools provided by a hosted applications vendor, the company recommends that its customers license CORE Impact to unleash real-world exploits on their computing infrastructure and staff through an aggressive penetration testing program.

“Penetration testing is the icing on the cake for vulnerability management, and CORE Impact allows you to assault your systems just as real attackers would to ensure that there’s no way to break in,” stated the CTO. “It shows you how real-world attacks play out against your defenses and illustrates how security controls are working, and where they’re breaking-down.”
Open-source pen testing tools may offer some ability to discover security weaknesses, but the CTO said that CORE Impact Pro provides customers with a more consistent methodology for tracking and analyzing vulnerabilities, one that can be used by staffers with varied levels of technical experience. As a commercial-grade security assessment package, CORE Impact provides the auditing and reporting tools that allow security teams to take action on the problems they find, and share that information with line-of-business leaders and compliance departments, or auditors.

Developed entirely in-house at CORE Security, the exploit code used in the product undergoes frequent and thorough quality assurance review, meaning that users can run regular tests against live infrastructure without jeopardizing systems integrity or introducing potential backdoors.

“With CORE Impact, we equip customers to continue to identify, reduce and manage their attack surfaces long after the consulting engagement is over. The solutions themselves can’t be stumbling blocks – rather, they must be enablers that offer usable results and fast learning curves.”

The Result

Lending long-term value to consulting engagements

Customers seek to gain tangible assets that will provide them with continued benefits long after their consulting arrangements have been completed. By encouraging organizations to adopt CORE Impact, consultants can provide organizations with a consistent, re-usable framework to utilize in furthering their own vulnerability management efforts.

The organization specifically markets its ability to offer continuous security assessment via its branded services, and by arming its customers with a solution in hand that allows them to self-analyze and audit their defenses on a regular basis, those organizations can formalize their vulnerability management programs and integrate pen testing into broader security strategies.

“We help customers transition from the annual assessment, audit and testing mentality to one of daily or weekly analysis,” said the CTO. “Our goal is to promote, equip, and train organizations with tools that provide security data at their fingertips.”

Validating vulnerability testing

Vulnerability scanning tools can provide organizations with reams of data about their weaknesses, but feeding the results of those applications into CORE Impact will give customers the ability to determine which issues represent their biggest risks, and how attackers will actually attempt to circumvent their defenses.

Penetration testing exercises carried out using CORE Impact allow companies to continually assess the efficacy of their network and endpoint filtering tools, including IPS, IDS, firewalls and AV systems.

Laying a foundation for user education training

As anti-virus vendors struggle to keep up with the appearance of new, more targeted threats, and attackers employ customized schemes aimed at victimizing specific sets of end users -- such as through spear-phishing -- it has become increasingly clear that employee security training programs represent organizations’ last, and most crucial, line of defense.

Using CORE Impact, customers can create multi-staged attacks that illustrate how well their employees adhere to security policies, and to craft plans for future end user education efforts. Consultants can work with organizations to investigate just where their policies are falling short, and use those results to cross-sell customers on future employee training engagements.

Driving maturation of customer security strategies

One of the organization’s biggest goals with its assessment services is to help customers move from a model of responsive security to one of proactive defense. By isolating where an organization’s security vulnerabilities lie using CORE Impact, customers can stop wondering where they may be exposed and start making strategic plans to address their real deficiencies. By embracing the entire vulnerability management process, companies can progress rapidly from under-informed alert responders to educated security planners.

“We’ll take a customer from merely being concerned that their network can be broken into, and responding to individual attacks, to strategically thinking about protecting sensitive information like credit card data and addressing specific aspects of compliance regulations,” said the CTO. “By adopting an end-to-end vulnerability management program that includes pen testing carried out via CORE Impact, customers can mature their entire security strategy quickly, and move from playing a game of catch-up to tackling emerging issues before they become real problems.”