SMARThER SECURITY FOR SmARThER THREATS

It’s a challenge to protect against today’s threats. They are targeted and take advantage of Zero-day vulnerabilities, go unrecognized by signature-based solutions, evade behavioral defenses via ‘low and slow’ attack profiles and are increasingly adaptive. Security analysts have determined that in-house resources alone are not enough. Websense® CyberSecurity Intelligence™ (CSI) services let your IT staff join forces with Websense Security Labs™ researchers to assume a more proactive security posture.

WHY WEBSENSE® CSI SERVICES?

Supercharge your IT staff with Websense CyberSecurity Intelligence (CSI) services and leverage Websense Security Labs researchers for an enhanced and effective security posture. CSI services offer a unique blend of in-depth security education, threat intelligence, expert consultations, real-time forensic investigation tools and more. Your organization will be better positioned to assess the unique risks its network may face based on recent threat activity or technology trends.

Prepare Your Network Against Targeted, Zero-day and Other Emerging Threats

- Ensure IT staff understand the technical details behind the risk potential of new technologies such as mobile devices.
- Get three days of training, including hands-on labs exercises, with Websense Security Labs™ researchers.
- Perform deep analysis of suspicious code using an on-demand behavioral sandbox and receive a detailed activity report of the results.
- Ensure optimal security architecture, configurations and policies through semi-annual reviews by Websense security experts.
- Have Websense researchers review your white/black lists and report on the current threat intelligence for each item.

Forensics through Behavioral Sandboxing

CSI services include access to an online sandbox environment for safely testing potential malware. Using Websense ACE (Advanced Classification Engine) analytics, all activity is monitored and documented in a detailed report including:

- The infection process
- Post-infection activities including network communications
- System-level events and processes
- Registry changes and file modifications

Observed behavior is correlated with known threats to provide valuable information for even Zero-day threats, all in real time.

“IT’s becoming clear that many of these emerging threats cannot be defended against in-house, creating a shift in security posture toward being more proactive.”

- Christine Liebert, Senior Analyst, IDC

THE WEBSENSE DIFFERENCE: ACE (ADVANCED CLASSIFICATION ENGINE)

Websense ACE provides real-time, inline contextual defenses for Web, Email, Data and Mobile security by using composite risk scoring and predictive analytics to deliver the most effective security available. It also provides containment by analyzing inbound and outbound traffic with data-aware defenses for industry-leading data theft protection. Classifiers for real-time security, data and content analysis — the result of years of research and development — enable ACE to detect more threats than traditional anti-virus engines every day (the proof is updated daily at http://securitylabs.websense.com). ACE is the primary defense behind all Websense TRITON® solutions and is supported by the Websense ThreatSeeker® Intelligence Cloud.

<table>
<thead>
<tr>
<th>Your Needs</th>
<th>Websense Solutions</th>
<th>CSI: On Demand</th>
<th>CSI: Live</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-depth security education</td>
<td>Online training provides on-demand access to security courses ranging from exposing encrypted code to troubleshooting compromised mobile devices. New courses are added based on current Websense Security Labs research projects.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Exclusive research presentations</td>
<td>Recordings of Technical Advisory Board (TAB) presentations, security industry lectures and other exclusive material designed for security professionals.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Malware analysis tools</td>
<td>CSI services include access to an online sandbox environment run by Websense Security Labs, for safely testing potential malware. Files are executed and a full, detailed report on observed behavior is provided, which includes any significant correlation with known threat activity.</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Hands-on security training</td>
<td>Websense Security Labs researchers will offer detailed, face-to-face security training events. These include intense hands-on labs exercises, and are designed to give attendees experience with threat scenarios and a unique networking opportunity.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Proactive defense consultation</td>
<td>Full, semi-annual review of security policy and configuration based on industry, regional and enterprise concerns, plus quarterly reviews of custom white lists/black lists that provide current categorization and threat classification information on each item.</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Incident investigation support</td>
<td>In the event of an actual security incident, CSI customers can call upon a Websense Security Labs researcher to assist with the investigation. It includes dissecting malware samples to identify how they function, tracing their origin, response and remediation strategies.</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

CONTACT US TO LEARN MORE: www.websense.com/Contact

© 2015 Websense, Inc. All rights reserved. Websense the Websense, TRITON and ThreatSeeker logos are registered trademarks of Websense, Inc. in the United States and various countries. All other trademarks are the property of their respective owner.

[DS-CSI-ENUS-13NOV14]