WireX Systems
Service Offerings for MSSP

Designed to address the biggest MSSP challenges

From an end customer's perspective, the most notable objection to MSSP is that MSSP personnel lack the required context and understanding of the end customer's environment to be truly effective in detecting and investigating an incident. The problem is even worse when looking at the transition many MSSPs are looking to do in order to become an MDR (Managed Detection and Response). The ability to perform deep investigations and recommend remediation activities that factor the operational impact of such actions is a core capability necessary in becoming an MDR. Without this, MSSPs are forced to provide lower priority services where it is hard to command a premium. Therefore, while most MSSP can actually capture revenue, it is still a struggle to gain profitability as the service becomes more a traditional labor outsourcing.

WireX Systems Network Detection & Response

WireX Systems' Network Detection & Response platform provides faster detection and investigation capabilities that turn even entry level operators into experienced tier-3 analysts. The platform is designed for all levels of security operations professionals that are tasked with responding to alerts and need to collect relevant data in order to understand the context and identify real threats. It is also a very powerful threat hunting tool for those who are offering advanced proactive services.

WireX Systems new service offerings for MSSP

Assessment - One time snapshot

One-time network snapshot report and recommendations.
Deploy WireX, run it for one week and get a report with the high, medium, low severity findings and recommendations.

Dynamic Breach Investigation Enablement (DBIE)

Deploy and leave WireX in the customer's environment as an insurance policy. At any time the customer can ask the MSSP to access the WireX platform to get full visibility and control on the situation. Note: the fee is just setting up WireX and permission to access it in case of an incident. No MSSP analyst time is included here, although it could be bundled in.

DBIE + Monthly report

All that is included in the DBIE service, plus a monthly report that contains:

1. High, medium & low severity findings.
2. Analysis of the customer's environment and trends over time.
3. Recommendations on situations that require further analysis or remediation.

DBIE + Monthly report + block of analyst hours

Deploy and leave the WireX platform in customer's environment. Get a monthly report with status & trends in high, medium & low severity findings. Use analyst hours to triage high severity alerts. Packages for analysts could include blocks of 100 hours, 200 hours and >400 hours.

DBIE + Monthly report + block of hours of investigators + remediation activities

With the MSSP having in-depth visibility into their end customers environments the ability to bundle in investigation actions along with advanced reporting and remediation activities for top severity incidents.

Threat Hunting

Block of hours of threat hunters proactively looking for suspicious behavior in the customer's environment. These could include ad-hoc activities upon having threat intelligence targeting a specific vertical as well as a proactive routine process.

[22ʅʎyƎ ΰ2 Y2ØŜ ₸₪2Y I-fŜ₪ΰă I-yŘ ăèYLJΰ2Yă ΰ2 ŘʌI-Ǝy2ăΰʌÔă I-yŘ ₪ŜYŜŘʌI-ΰʌ2yK

Find out how WireX Systems solutions can help you. Contact sales@extralink.com

EXTRALINK

wirex