Field test with OpenDXL

solutionIT

Partner Profile:
IT security service provider, Bad Oldesloe/ Germany, with more than 15 years of experience in the security sector.

IT Environment:
The company has many years of expertise, including in networks and gateway security products.

The consultants and technicians from solutionIT support customers from a wide variety of branches and in different sized companies.

The team offers analyses and concepts as well as implementation of IT infrastructures and networks.

IT security is a team game: a company can enjoy comprehensive protection if information on threats is shared. For this reason, solutionIT security experts use Data Exchange Layer (DXL) in order to integrate solutions from different vendors.

Based in the northern German town of Bad Oldesloe, solutionIT GmbH is a systems vendor and consulting firm which focuses on IT security. Staff offer Germany-wide support for companies large and small, and from all industries—comprising comprehensive IT service, from analysis to strategy development, to implementation and support of IT infrastructures and enterprise networks. One of solutionIT's core tasks is ensuring IT security for customers. In doing so, the consultants frequently face the challenge of coordinating multiple security systems within one enterprise network.

"Companies can buy into the best firewalls and most expensive web gateways, but neither can unfold their full potential until they are networked," explains Olaf Otahal, CEO of solutionIT. "When a firewall registers a threat, this information has to be shared. Otherwise the other systems remain blind to the threat, and the attacker is at an advantage."

Sharing threat information

For 15 years, solutionIT has partnered closely with McAfee. When the McAfee began to take a new open source approach in 2016 with Data Exchange Layer (DXL), solutionIT saw it as the perfect opportunity to integrate security systems in practice. The Data Exchange Layer enables different security systems within one and the same company to share information, regardless of make. In doing so, the information is not only shared via the DXL interface, but also augmented and prepared for further processing.

"We consider the Data Exchange Layer the answer to our quest for better networking between different security systems," explains Otahal. "When the interface opened with OpenDXL, we saw that the time had come to test the system in practice. And I must say—we're delighted with the results! The flexibility and structured simplicity when working with OpenDXL is impressive. For us, integration of this kind adds considerable value to the support we are able to offer our customers, which in turn increases customer loyalty."

Field test with OpenDXL

At the end of 2016, solutionIT began with implementation, initially as a demonstration in a standard environment for customers. The Data Exchange Layer was quickly installed and showed a Store&Forward and a Push integration from McAfee products and a Forcepoint firewall where you could see automatically generated security threats being thwarted in real time.

In the Store&Forward integration, notifications on malicious IP addresses, URLs, and hash values as well as situational notifications (on DDoS attacks, for example) are collected centrally in a Threat Intelligence platform. In this manner, the individual pieces of information can be assigned to different security vectors. This enables companies to build up threat databases which they can share internally or even externally with other companies.

The direct OpenDXL integration approach does not have interim storage. Instead, all accessible network components are protected within a very short space

How OpenDXL works

In this example, a company secures its infrastructure via a firewall. This registers all attacks, whether internal or external, and blocks external attacks—from Port Scan to Exploits to DoS attacks. This is traditionally where the firewall's job ends, even though the information it has registered—e.g., the type of attack or the attacker's IP—is highly valuable. To date, however, no further use was made of this information.

With the Data Exchange Layer, information can now be forwarded downstream to systems where it is assessed. These insights can be augmented and mirrored back, so that the firewall can use it, for example, to complete an automatic block list with IPs from the attacker's source area. This enables the firewall to counter future attacks more swiftly. On the other hand, the insights can also be forwarded to other systems which have a DXL interface—a web gateway, for example—which then prohibits clients from accessing the dubious IP addresses. In this manner, information on threats can be shared and augmented regardless of manufacturer, and help to comprehensively protect the infrastructure. The sole requirement: each individual system needs to have a DXL interface.

of time. For this purpose, the central Forcepoint SMC (Security Management Center) is able, for example, to forward IP addresses directly to the McAfee web gateway and the McAfee TIE server. By passing the information on to the TIE server, all existing McAfee security solutions are then also automatically informed.

"DXL increases our security, and the augmented threat information is another protection criterion for us. We would be acting negligently were we not to make use of these advantages ourselves—we were quickly convinced of the efficacy of the OpenDXL standard. Hence we quickly moved from a test environment to a production environment," explains Otahal.

solutionIT customers were also quick to appreciate the added benefits. Networking their existing security systems not only ensures a high level of protection, but also a high degree of automation for their IT security. And the approach requires neither large investments nor undue effort.

The advantage of openness: OpenDXL is increasing in demand

"We've received a strong increase in customer interest in recent months. Thanks to OpenDXL, connecting solutions via DXL interfaces has become universal—which in turn has made the entire system more efficient. Because in a best-case scenario, comprehensive security means the whole system is connected," adds Otahal.

solutionIT predicts strong growth in the future for OpenDXL. Hence the plan is not only to port DXL systems for customers, but also to further develop the standard environment—with additional threat scenarios, new interactions, and proactive measures for certain events. There is also talk of integrating McAfee Advanced Web Defense. In this manner, McAfee and solutionIT continue to develop and perfect all-round protection for companies, adapting this continually to the latest threats.

The future is exciting

Stephan Lehniger, Channel Technical Manager, looks ahead: "Together with solutionIT, a long-standing, active, and loyal partner, we have laid the foundation for a new dimension of collaboration: the potential from multi- and single-vendor integration can exponentially increase the current standards of security environments and the level of security they offer. In our work with our partners, we focus on enabling customers to combine the various solutions and access these added benefits, and I can hardly wait to see the various executable environments we'll have in the field in a few months' time."

McAfee™
Together is power.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com