Press release

Managed Endpoint Detection & Response from Swisscom delivers greater security to companies

Laptops, desktops and smartphones are the focus for cyber criminals. Preventative measures on their own are not enough to stop them. To respond to sophisticated cyber attacks, additional protective measures are needed, such as an Endpoint Detection & Response (EDR) system. Swisscom is launching a new managed service for businesses.

It often starts with the end device: endpoints – laptops, PCs, smartphones and local servers on the corporate network – are the initial point of entry in around 70 percent of cyber attacks. This is the conclusion of a study by the US security provider ‘Absolute Software’. Attacks are becoming increasingly sophisticated, with notable rises in fileless attacks, which may be present in programming code and run exclusively in the computer’s RAM, leaving no trace in the file system. “Attacks such as these go unnoticed by most antivirus programs and are not even recognised by firewalls,” explains Cyrill Peter, Head of Enterprise Security Services at Swisscom. “It is therefore vital to give devices additional protection to ensure that attacks can be detected and prevented swiftly.”

The final piece in a comprehensive security solution

Endpoint Detection & Response (EDR) is the answer. Unlike signature-based antivirus software, EDR analyses device behaviour and looks for anomalies. “The dashboard allows our customers to track everything in real time,” says Peter. “This ensures that potential security vulnerabilities can be revealed across all end devices. Security alerts are automatically investigated and resolved where possible, which frees up the security operations team.”

However, EDR does not automatically detect and prevent all attacks. EDR needs to be integrated into overarching security solutions and embedded into a Security Operation Center (SOC), and experienced security analysts often need to evaluate suspicious endpoint behaviour. With EDR, analysts can focus on a smaller number of suspected attacks (handled alerts) and do not have to evaluate thousands of events and logs, massively reducing their workload. If an incident does occur, EDR gives the security team a rapid overview of the monitored IT infrastructure and enables them to respond immediately across all the endpoints, by isolating an endpoint compromised by malware or by moving suspicious files into a quarantine directory.

EDR is therefore not a standalone solution and should be integrated into existing security solutions and processes. EDR from Swisscom can be combined with SOC as a Service or CSIRT as a Service, for instance. This allows Swisscom customers to mount a successful defence against fileless attacks such as malware, invasive programs and zero-day exploits.

How Endpoint Detection & Response works

Devices connected to networks provide potential targets for complex cyber attacks as the endpoints in a network. Endpoint Detection & Response (EDR) monitors all the activities on the endpoint in real time, including those transferred to the network, and automatically checks and resolves security alerts, thus protecting all the network access points from complex cyber attacks.

White paper:
https://www.swisscom.ch/en/business/enterprise/downloads/security/endpoint-detection-response.html

EDR product website:
https://www.swisscom.ch/en/business/enterprise/offer/security/edr.html

SOC Services product website:
https://www.swisscom.ch/en/business/enterprise/offer/security/threat-detection-and-response.html

Berne, 14 October 2020