Managed Detection and Response

Effective protection through a comprehensive SOC service bundled with endpoint security

Businesses need more than traditional security

The number of cyber attacks is continuously increasing. Not just that, but the complexity of attacks is also constantly growing. Hence, detecting an attack becomes complicated.

The consequences range from data theft and operational downtime to espionage and financial losses. But the company's image is at stake too. Any kind of reputational damage affects revenues in the long run.

One thing is clear: the costs in the event of an attack are serious. Conventional firewalls and antivirus solutions are not sufficient to adequately protect corporate assets. Why? They are efficient in protecting against known threats, but there are chances that unknown threats emerging from outside the perimeter will go undetected. At the same time, however, there is often a lack of time and money to implement holistic security projects.

Solution: Endpoint Detection and Response

An Endpoint Detection and Response (EDR) solution is more sophisticated than antivirus software. It includes antivirus capabilities plus powerful functionality such as advanced persistent threat (APT) detection, advanced analytics, response mechanisms, device management, and more. For instance, if an endpoint is infected, EDR will trigger an alert, isolate the endpoint, and provide forensic information to security teams for incident analysis.

But EDR demands manual intervention and it's a half-baked solution if you don't have expert teams to intervene.
This is why Managed Detection and Response (MDR) is needed.

How MDR can help you to build the right defense:

- Full-scale SOC with continuous analysis
- Ability to trigger and perform response measures
- Regular review processes and threat hunting to detect sophisticated attackers
- Weekly consultation from our security experts and continuous improvement of your security level
- More than 20 years of experience in security projects

T Systems

Let's power higher performance

MDR: Components of your cyber security perfectly combined

T-Systems Security Operations Center

Continuously analyzes suspicious activities

1. Access to the insights from the SOC
2. Real-time data and reports on the current security status
3. Weekly consultation sessions about the status and improvements
4. Real-time support for security incidents

Protection: Endpoint Protection

Blocks the execution of suspicious files or processes

1. Protection of all clients and server endpoints
2. State-of-the-art security solutions enable multi-level protection mechanisms
3. Machine learning algorithms prevent the execution of malicious processes, and threats can be detected and averted at an early stage
4. Central management platform enables security analysis and replaces the existing anti-virus solution

Detection: EDR and SOC

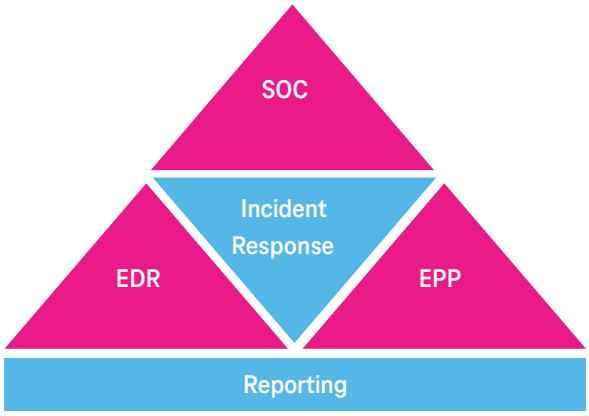
Collects process information for analysis by SOC experts

1. Review and triage of alerts to determine the severity of attack and recommended action
2. Continuous finetuning to reduce false positives
3. In-depth analysis of processes causing suspicious behavior
4. Remote sessions on endpoints for advanced analysis and hunting via EDR
5. Regular threat hunting to investigate potentially existing compromises and find sophisticated low-profile attackers that avoid generating alerts

Response: EDR and Incident Response

Initiates of countermeasures in the event of an attack

1. SOC triggers response measures remotely based on analysis results such as isolation of hosts, stopping of processes, and blocking of executables
2. The incident response team responds to large-scale compromises



EDR: Endpoint Detection and Response EPP: Endpoint Protection
SOC: Security Operations Center

When you should consider MDR

- You have limited resources internally
- Your level of security expertise in the company is limited
- Your current EDR solutions cannot detect advanced threats
- Your existing security levels still have to develop and mature
- Above all, you want to focus on your core business and strategic initiatives

Trusted by businesses for one of the best-in-class MDR services.

Expert contact

Andreas Pecka
Head of International Expert Sales
& Presales - Cyber Security
a.pecka@t-systems.com

Published by

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Germany
E-Mail: cyber.security@t-systems. com
Internet: www.t-systems.com

Last update: 04/2023

T Systems

Let's power
higher performance