Strengthening the security with XDR / MDR In Practice

Attacks are becoming more sophisticated and destructive

Increase in the number of threats

Complex attack scenarios

Financial damage caused by attacks

Shortage of qualified specialists

Failure to process alerts quickly

Enterprise security trends: External Factors

Most advanced threats using basic vulnerabilities and human factor

Availability and lowering prices leading to Cybercrime-as-a-Service

Attacks on third-party: SMBs can become a part of an attack chain

Enterprise security trends: Internal Factors

Growing IT sophistication results in visibility gap and lack of operational information

An average targeted attack stays undetected for more than 214 days

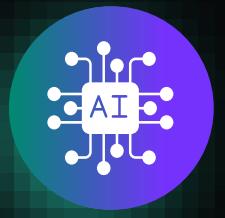
Perimeter security is overestimated

AI In the Wrong Hands...

AI-Assisted
Social Engineering

AI-Automated Scam &
Fraud Operations

AI-Generated
Malware



LLM
Exploitation

Just look at the numbers!

467,000	unique malicious objects discovered by Kaspersky every single day
>900	APT groups and operations
>2 billion	attacks launched from online resources around the world blocked by us
38.6%	of ICS computers globally have been attacked
1 billion	devices protected by Kaspersky to date

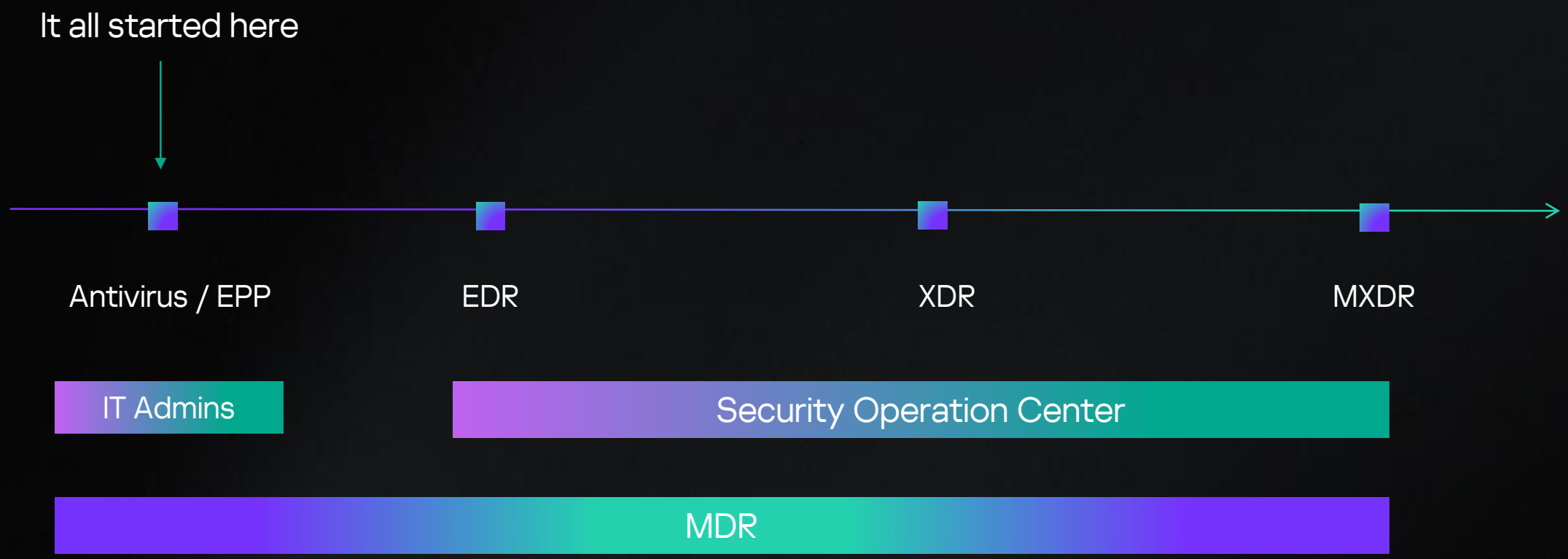
Evolving cybersecurity challenges

- Siloed tools - Fragmented visibility
- Poor prioritization of security alerts coming from multiple security technologies
- Analyst burnout, increasing staff turnover rates
- Inefficient incident response, leading to high recovery costs
- Undiscovered threats lurking within the organization
- Lack of a comprehensive threat overview, impeding efficient security program development
- MTTD* & MTTR** is too high

*Mean Time To Detect

**Mean Time To Respond

Evolution..


It all started here
Antivirus / EPP
EDR
XDR
MXDR
IT Admins
Security Operation Center
MDR

What does XDR mean in practice...

Cross-platform correlation

XDR Correlates data across endpoints, networks, cloud, email, and identity to detect and respond to threats faster and more accurately

- Unified Visibility
- Cross-domain correlation
- Data Lake
- Automation – investigation & Response
- Reduce MTTD & MTTR

Kaspersky XDR Practical Capabilities

Focus on outcomes, not just features

- Centralized detection across multiple vectors
- Advanced Analytics + threat intelligence
- Automated (Playbooks) and guide response actions (MDR / AI powered)
- Advanced case management
- Open architecture (integration with existing tools)
- Leverage data sovereignty
- Monitor every device on the network – EPP & EDR
- Hybrid environment security
- AI Asset scoring

Uncovering previously unknown iOS Malware

Operation Triangulation (June, 2023)

While monitoring the network traffic of our own corporate Wi-Fi network for mobile devices using our XDR cross-correlation engine, we noticed suspicious activity that originated from several iOS-based phones.

MDR – Addressing the challenges

Why MDR is becoming essential

- Threat landscape is evolving – The complexity of modern threats
- Advancement in attack tools & techniques by leveraging AI
- SOC analyst skills/expertise shortage
- Attacks don’t sleep – 24 / 7 monitoring required

Technology alone is not enough

Kaspersky MDR – Practical capabilities

Clear and practical

- 24/7 Monitoring by Kaspersky Experts + AI powered
- Continuous Threat hunting and incident validation
- Guided and/or full managed response (Change on demand)
- Advanced reporting and recommendations
- You are not alone – Direct Communication with Analyst
- Native integrations, additionally it works alongside with third-party systems

Security with and without MDR (Reason of request)

Impact is evident

Attack complete:

- Although there were related security alerts (Could have revealed the attack, if analyzed)
- No one to monitor the alerts
- Lack of MDR
- Low security awareness

Files encrypted	41.6%
Data leakage	16.9%
Defacement	1.7%
Money theft	0.6%
Service unavailable	0.6%

Suspicious activity was detected

Post compromise, before impact:

- Investigation started after detecting alerts
- Mostly in earlier phases of attack
- Small detection can lead to revealing an APT attack
- No impact, or lowest possible, with containment after compromise
- MDR is active, either by local resources or provided by Kaspersky
- Some turned out to be FA. But, better safe than sorry

Persistence installed for future impact	10.7%
Active Directory compromised	9.6%
None (False alarm)	5.6%
Account takeover	4.5%
None (Attack prevented or not finished)	4.5%
Data Destruction	3.4%
Data manipulation	0.6%

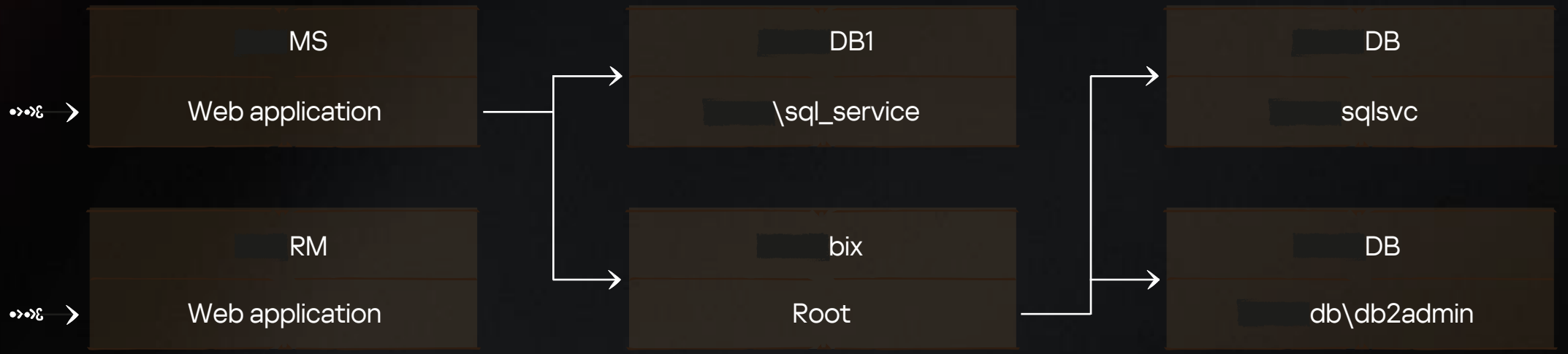
Case (Importance of MDR)

MDR report with suspicious activities discovered in the Customer's network (Old web-shells)

MDR was deployed after the upload of web-shells

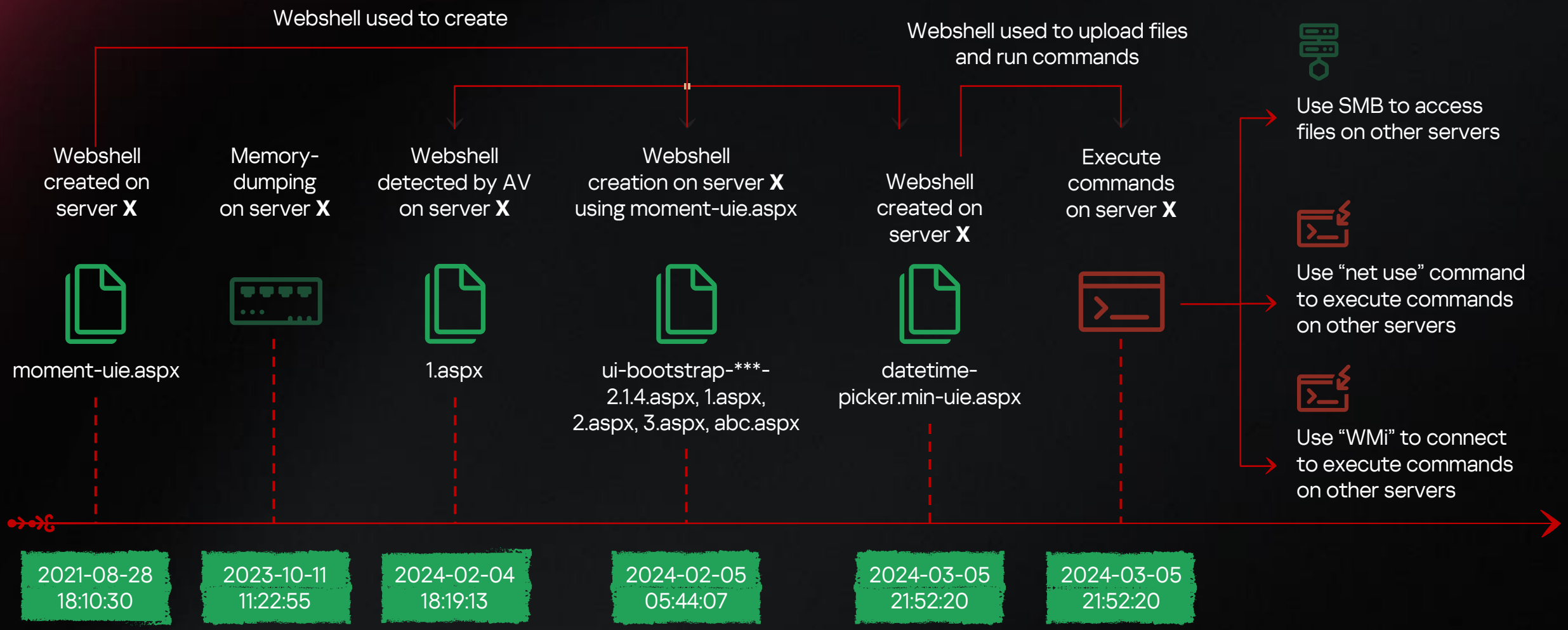
IR investigation started, confirming the compromise and exploiting existing vulnerability

Adversaries had different lateral movements



The attack was stopped before impact thanks to the early alert and action from MDR

Case: APT attack (Long-lasting – Telecom)



XDR vs MDR?

XDR

- Technology & Platform
- In-house control & visibility
- Automation

MDR

- People + Process
- Outsourced Expertise
- Human-led and AI investigation

Value for Organizations

- Reduce MTTR and breach impact
- Improved cyber resiliency
- Overcome skill/expertise shortage
- Always-on Service
- Free up your teams to focus on strategic initiatives