Angriff erfolgreich abgewehrt:
Success Story von Jo-Soft IT-Security & Kaspersky

Jan Oberbanscheid
Cybersecurity Consultant
Jo-Soft GmbH

kaspersky

[jo-soft]
IT-Security

Jan Oberbanscheid

Cybersecurity Consultant bei der

Jo-Soft GmbH

[jo-soft]
IT-Security

Agenda

Kaspersky Managed Detection and Response

Kundensituation

Die zwei Incidents

Aufarbeitung

Erfahrungen

[jo-soft]
IT Security

Über Kaspersky Managed Detection and Response

Managed Detection and Response-Lösung

Security Operations Center 24x7- Service

Schnellere Erkennung von Bedrohungen

Kompatibel mit anderen Endpoint Security-Lösungen

[jo-soft]
IT Security

Kundensituation

Produzierendes Gewerbe in der Automobilbranche

4.000+ Windows-Systeme

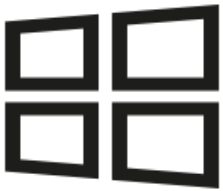
150+ Standorte weltweit

Verschiedene Lösungen im Einsatz

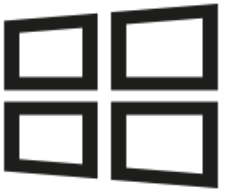
[jo-soft]
IT Security

Erster Incident

Username and
Password Guessing

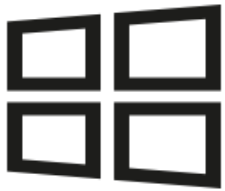


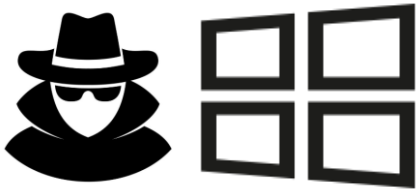
Erfolgreiche Verbindung



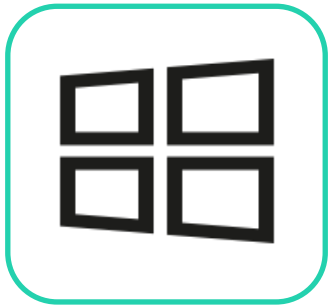
Erster Incident

Privilege Escalation

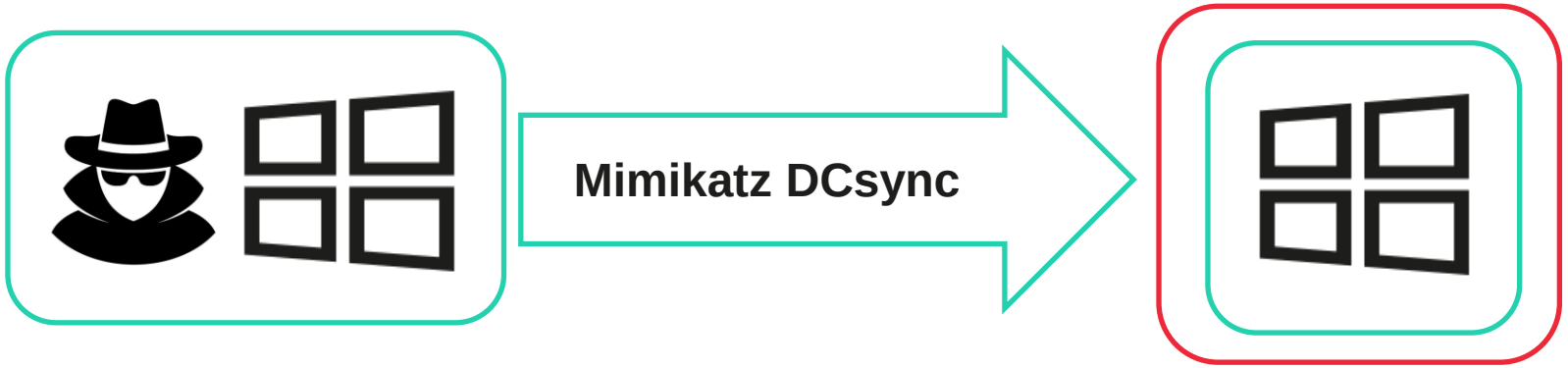




Lateral Movement



Erster Incident



Zweiter Incident

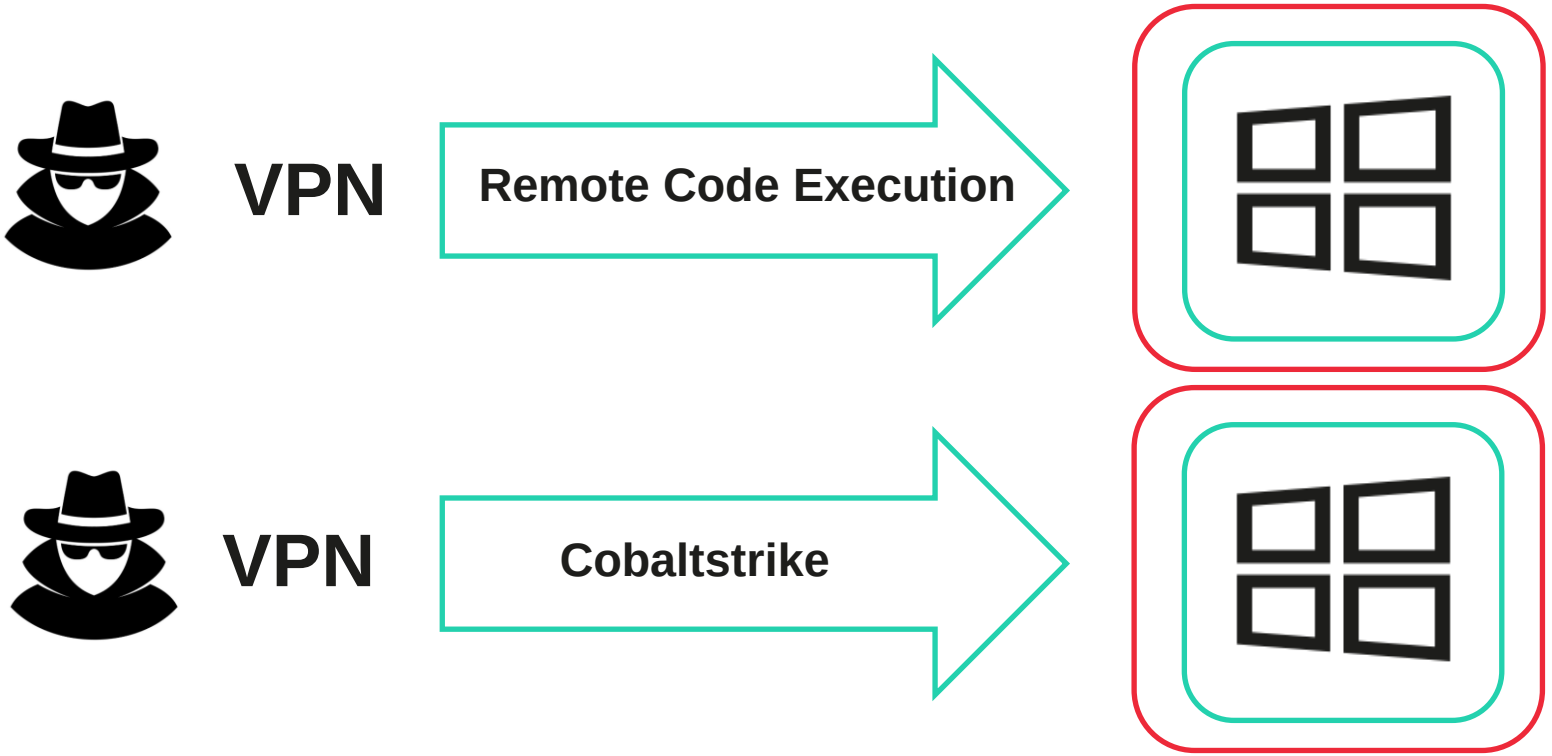
Credential Stuffing

VPN

Erfolgreiche Verbindung

VPN

Zweiter Incident



Aufarbeitung mit dem Kaspersky Global Emergency Response Team (GERT)

- **Analyse aller Clients und Server**, die mit den Angriffen in Verbindung gebracht werden konnten
- **Prüfung und Freigabe** betriebskritischer Systeme
- **Umsetzung von Handlungs-empfehlungen**
- **Dark Web Research**

Was wäre, wenn …?

Datendiebstahl

Systemausfall

Finanzieller Schaden durch Ransom-Zahlung

Produktionsstopp

Konventionalstrafen

Kundenverlust

[jo-soft]
IT Security

Erfahrungen

Flächendeckender Einsatz von Kaspersky MDR

Technische und Organisatiorische Maßnahmen

Penetration Testing

[io-soft]
IT-Security

als Partner

Koordination der Kommunikation

Unterstützung bei der Umsetzung von Maßnahmen

Planung weiterer Maßnahmen zur Prävention

Vielen Dank!

Besuchen Sie uns auf unserem Stand

Halle 7 Stand 7-310

[jo-soft]
IT Security

kaspersky