



Microsoft Ansatz zur Cyberresilienz: IT-Infrastruktur schrittweise und kontinuierlich widerstandsfähig machen

Nancy Mustapic
Technical Specialist Security

Tom Maier
Technical Specialist Security



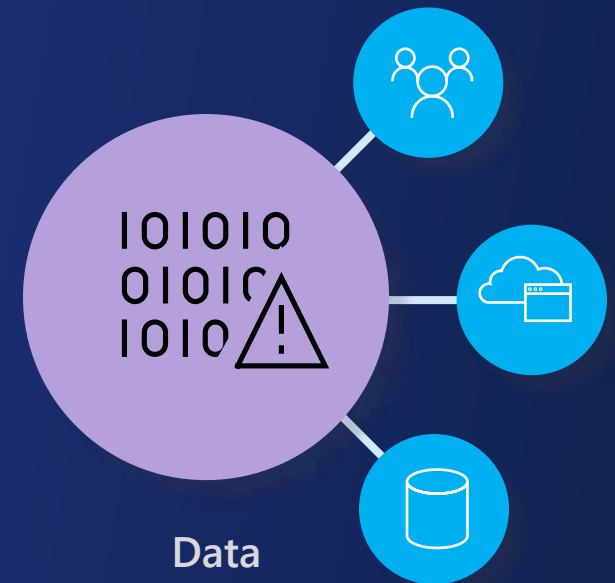
Ausgeklügelte Angriffe erstrecken sich über die gesamte IT Infrastruktur



Human-operated
ransomware campaign



Business email
compromise campaign



Data
exfiltration



Email



Endpoints



Identities



SaaS apps



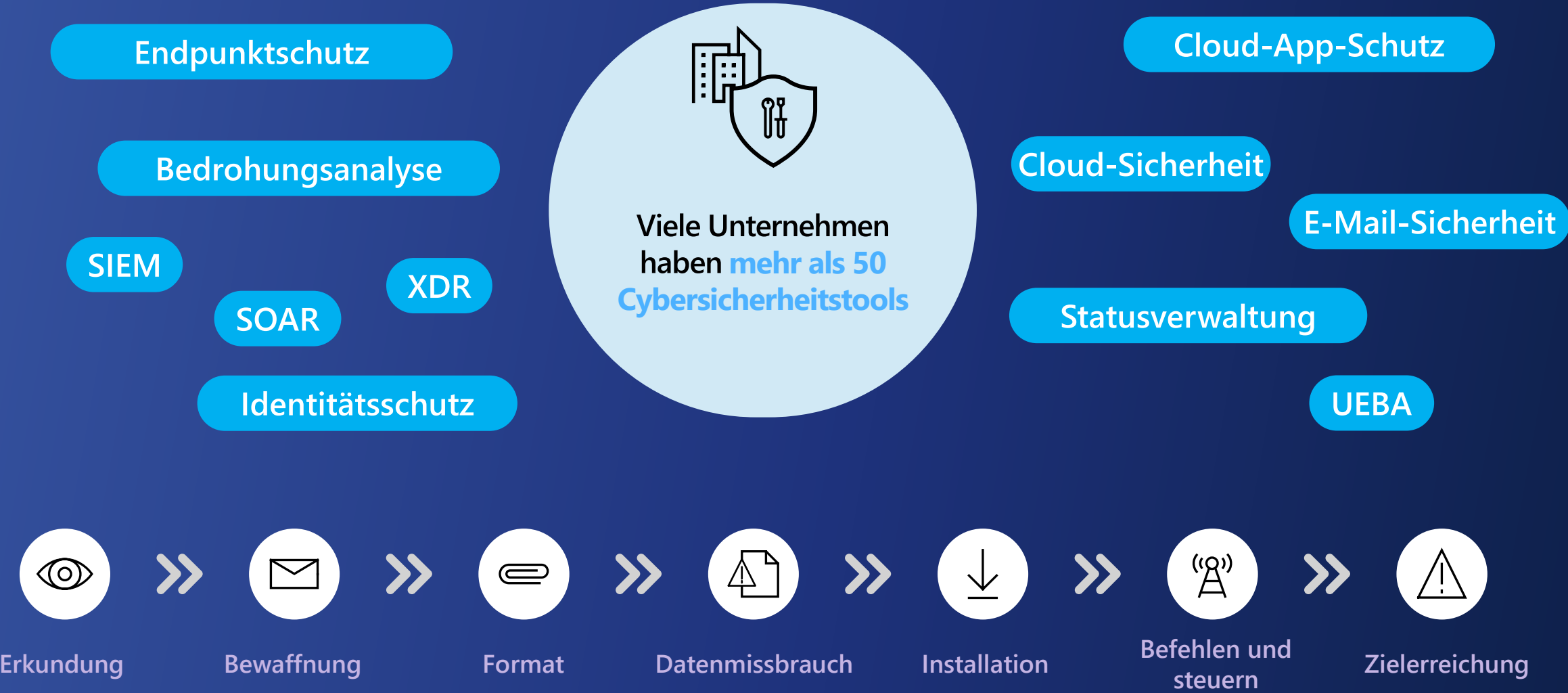
Data



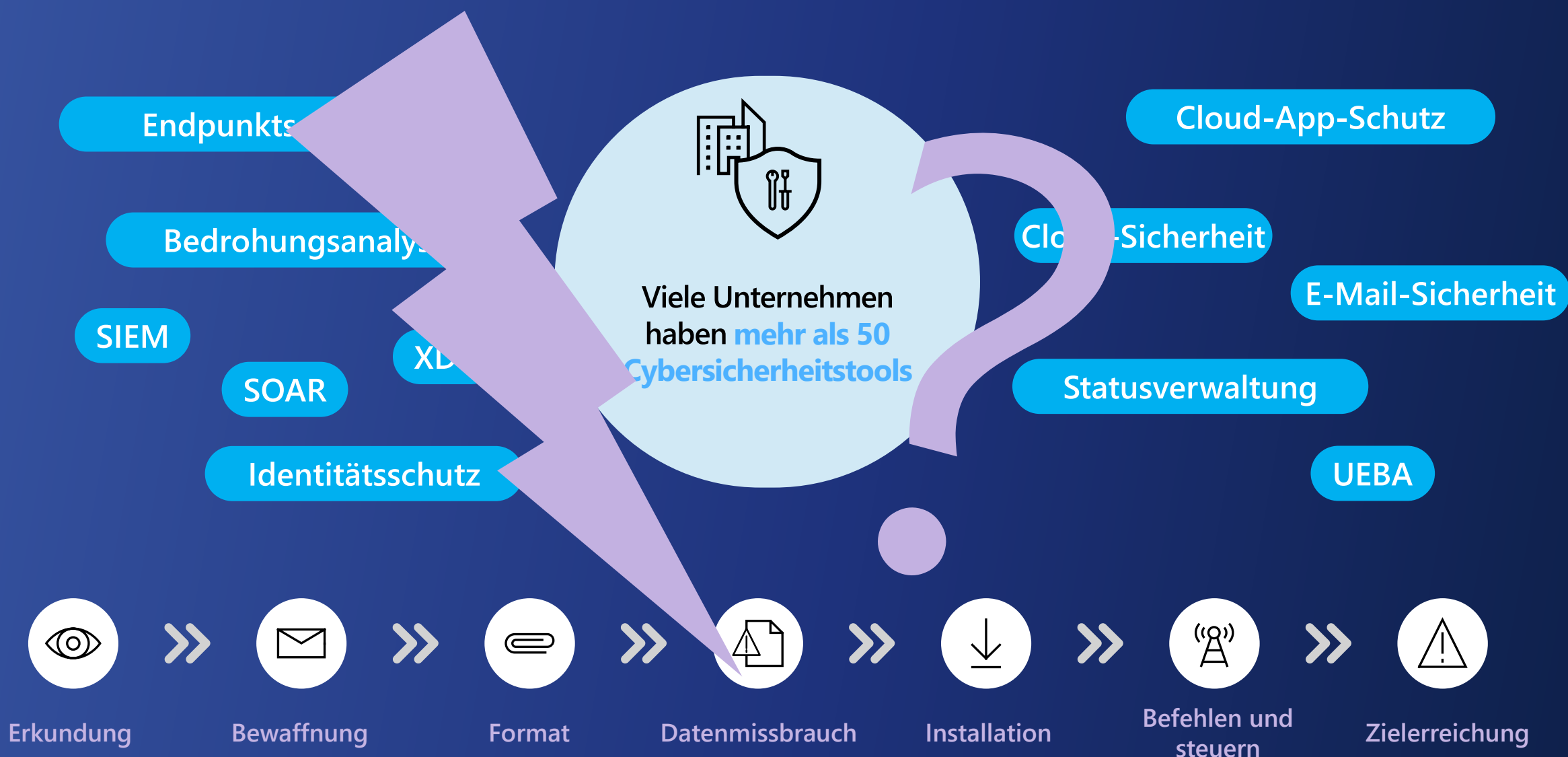
Cloud workloads



Heterogene, isolierte Sicherheitstools reichen nicht aus



Heterogene, isolierte Sicherheitstools reichen nicht aus



Schrittweiser Ausbau zur Cyberresilienz durch Tooling Strategy

XDR + SIEM + Security Data Lake

XDR – Deep Asset-Specific Tooling



ENDPOINTS
IT, IoT, OT



EMAIL



IDENTITY



APPS



MULTI-CLOUD & HYBRID CLOUD

Schrittweiser Ausbau zur Cyberresilienz durch Tooling Strategy

XDR + SIEM + Security Data Lake

SIEM – Broad Visibility & Correlation

XDR – Deep Asset-Specific Tooling



ENDPOINTS
IT, IoT, OT



EMAIL



IDENTITY



APPS



MULTI-CLOUD & HYBRID CLOUD

Other Data Sources

Event Logs from Devices, Services, Security Tools, etc.



NETWORK



**CUSTOM
APPS**



OTHER

Schrittweiser Ausbau zur Cyberresilienz durch Tooling Strategy

XDR + SIEM + Security Data Lake

Security Data Lake – Complete Record

Azure Data Explorer (ADX)

SIEM – Broad Visibility & Correlation

Microsoft Sentinel

XDR – Deep Asset-Specific Tooling



ENDPOINTS
IT, IoT, OT



EMAIL



IDENTITY



APPS



MULTI-CLOUD & HYBRID CLOUD

Microsoft Defender XDR

Microsoft Defender for Cloud

Other Data Sources

Event Logs from Devices, Services, Security Tools, etc.



NETWORK



**CUSTOM
APPS**



OTHER

Schrittweiser Ausbau zur Cyberresilienz durch Tooling Strategy

XDR + SIEM + Security Data Lake

Security Data Lake – Complete Record

Azure Data Explorer (ADX)

SIEM – Broad Visibility & Correlation

Microsoft Sentinel

XDR – Deep Asset-Specific Tooling



ENDPOINTS
IT, IoT, OT



EMAIL



IDENTITY



APPS



MULTI-CLOUD & HYBRID CLOUD

Microsoft Defender XDR

Microsoft Defender for Cloud

Other Data Sources

Event Logs from Devices, Services, Security Tools, etc.



NETWORK



**CUSTOM
APPS**



OTHER

Key Enablers

**Copilot for
Security**



**Behavioral
Analytics (UEBA)**

**Orchestration &
Automation (SOAR)**

Thank you!



Nancy Mustapic
Technical Specialist Security

Security Expert & Event Speaker
at Microsoft, Industry Expert for
Automotive & Financial Services



Tom Maier
Technical Specialist Security

Technical Specialist at Microsoft for
Public Sector & Defense Industry

