base it

professional.
fast.
secure.

PATRICK BÖCK

PATRICK.BOECK@BASEIT.AT

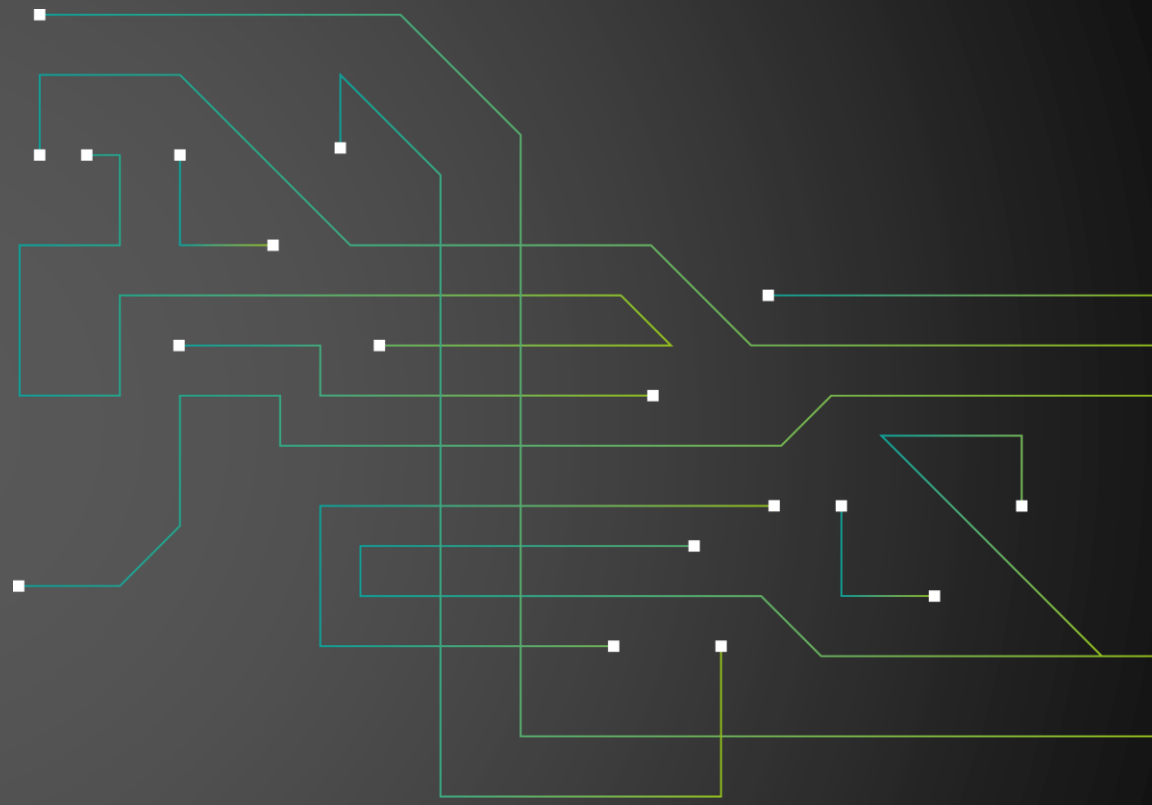
LEAD ARCHITECT MODERN WORKPLACE & SECURITY

professional.
fast.
secure.

AGENDA

base it

- ZIELGRUPPE MDATP
- ÜBERSICHT DEFENDER ATP
- LIVE DEMO DEFENDER ATP
- WHATS NEW MDATP
- ANPASSUNGEN & FEATURES



professional.
fast.
secure.

ZIELGRUPPE MDATP

base it

Aug 16, 2017, 11:47am EDT

NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million

Lee Mathews Senior Contributor

Cybersecurity

Observing, pondering, and writing about tech. Generally in that order.

NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs

The shipping giant has suffered millions of dollars in damage due to the ransomware attack.

NETZPOLITIK

Ransomware: Universität zahlte über eine Million Dollar, um Forschung zu retten

Server des Medizin-Instituts waren von einem Trojaner verschlüsselt worden, Verantwortliche sahen keine Alternative und verhandelten den Betrag hinunter

1. Juli 2020, 13:19 222 Postings

University of California SF pays ransomware hackers $1.14 million to salvage research

The malware infected crucial research stored in the UCSF medical school's network.

Travelex Paid $2.3 Million to Ransomware Gang: Report

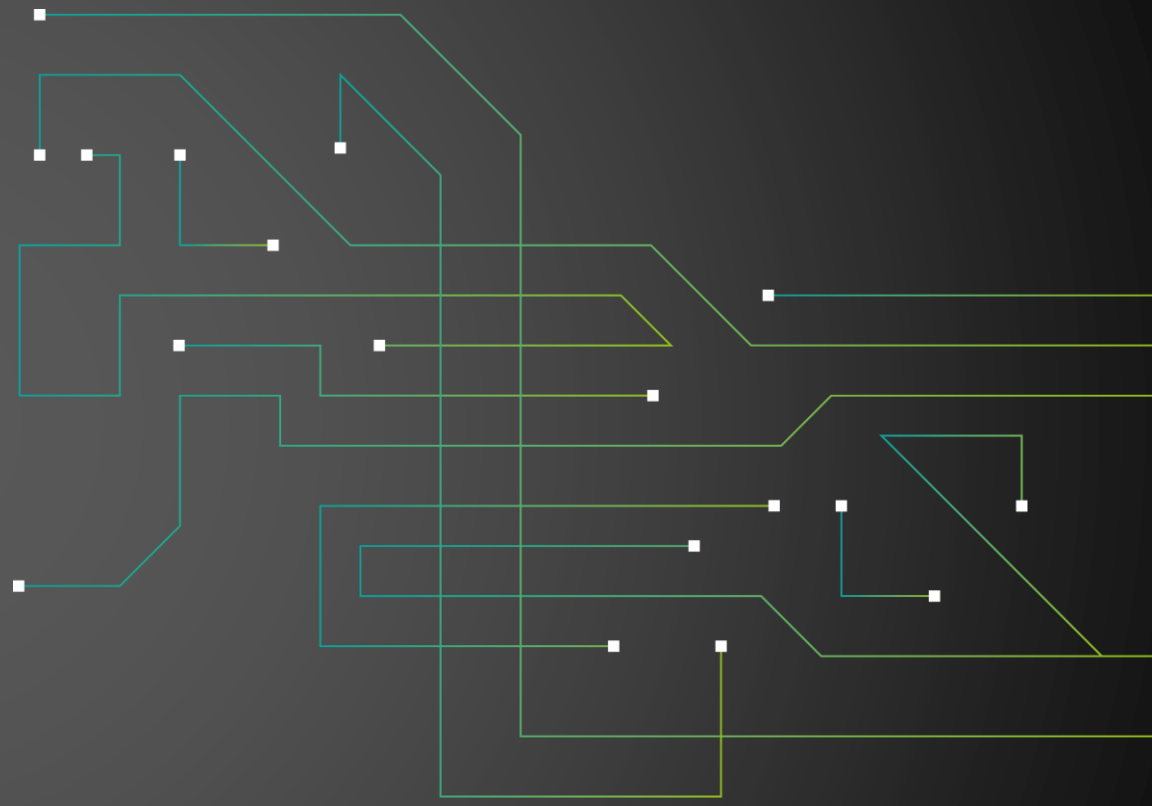
Attack Crippled Currency Exchange's Services for Weeks

professional.
fast.
secure.

ZIELSETZUNG

base it

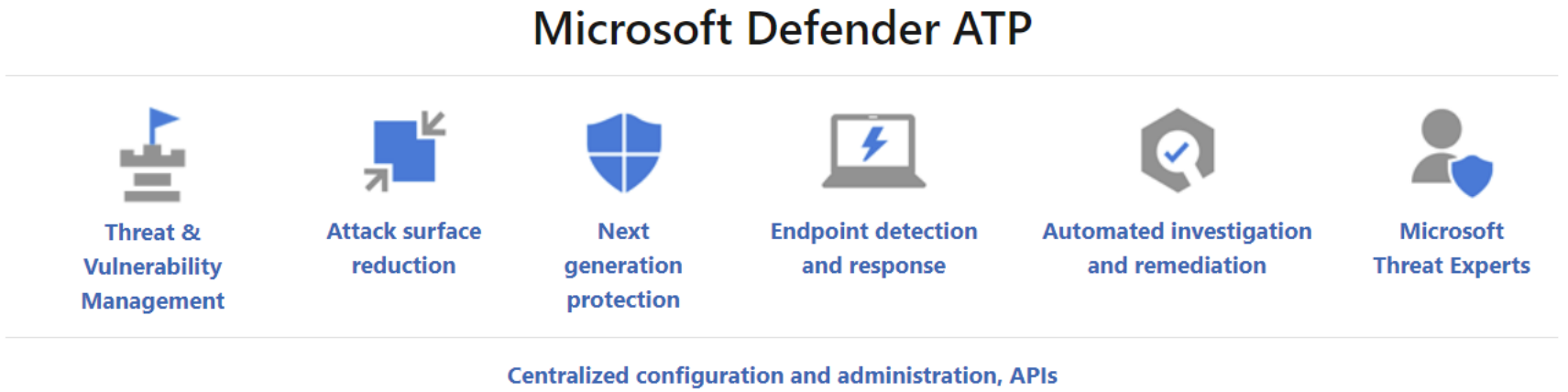
- ERKENBARKEIT (VISIBILITY)
- WIDERSTANDSFÄHIGKEIT (RESILIENZ)
- REAKTION (TIME TO ACTION)
- AUTOMATISIERUNG
- AWARENESS
- NACHVOLLZIEHBARKEIT



professional.
fast.
secure.

MICROSOFT DEFENDER ATP: OVERVIEW

TP
Defender ATP



Microsoft Defender ATP uses the following combination of technology built into Windows 10 and Microsoft's robust cloud service:

•**Endpoint behavioral sensors**: Embedded in Windows 10, these sensors collect and process behavioral signals from the operating system and sends this sensor data to your private, isolated, cloud instance of Microsoft Defender ATP.

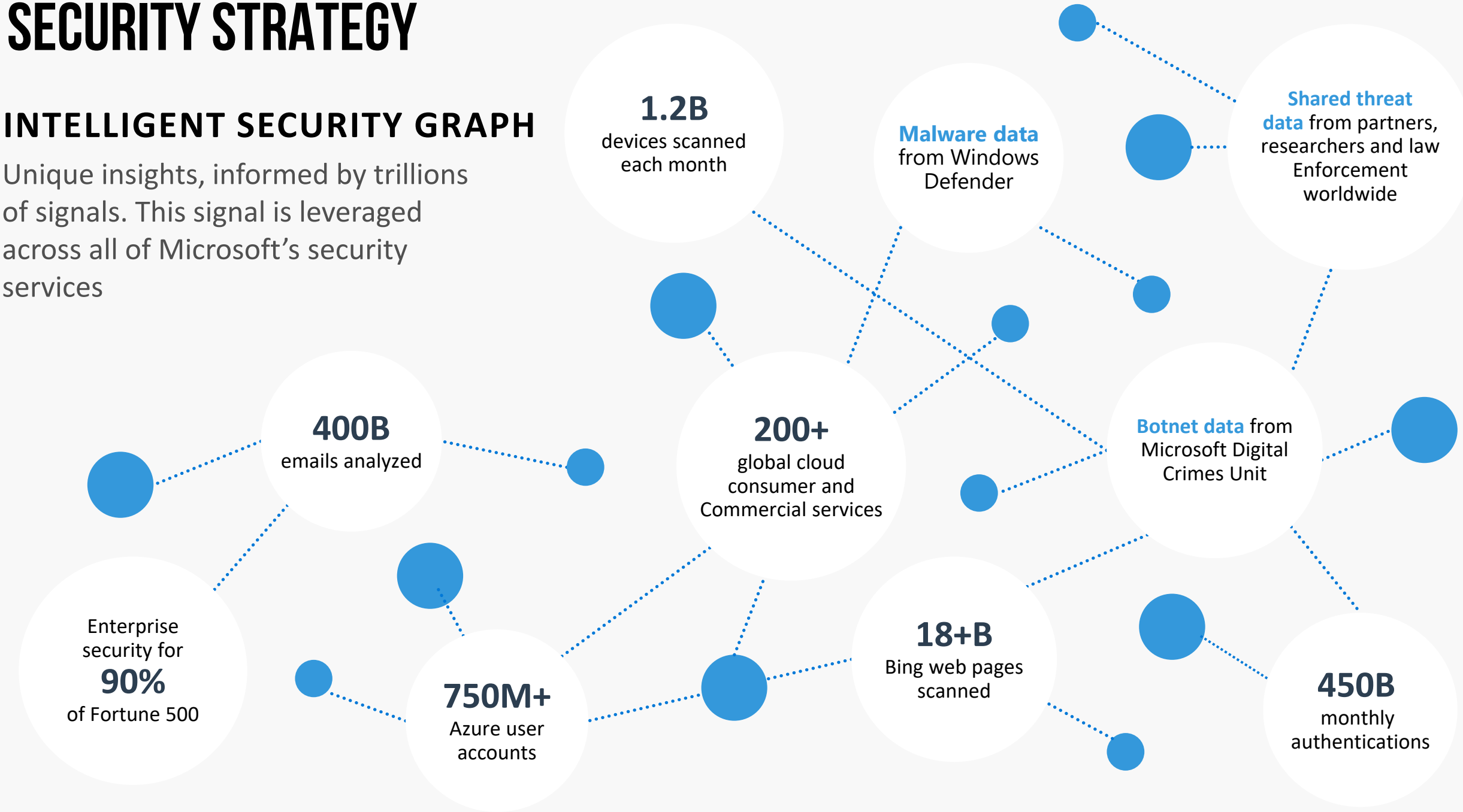
•**Cloud security analytics**: Leveraging big-data, machine-learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products (such as Office 365), and online assets, behavioral signals are translated into insights, detections, and recommended responses to advanced threats.

•**Threat intelligence**: Generated by Microsoft hunters, security teams, and augmented by threat intelligence provided by partners, threat intelligence enables Microsoft Defender ATP to identify attacker tools, techniques, and procedures, and generate alerts when these are observed in collected sensor data.

SECURITY STRATEGY

INTELLIGENT SECURITY GRAPH

Unique insights, informed by trillions of signals. This signal is leveraged across all of Microsoft's security services



DEVICE SUPPORT

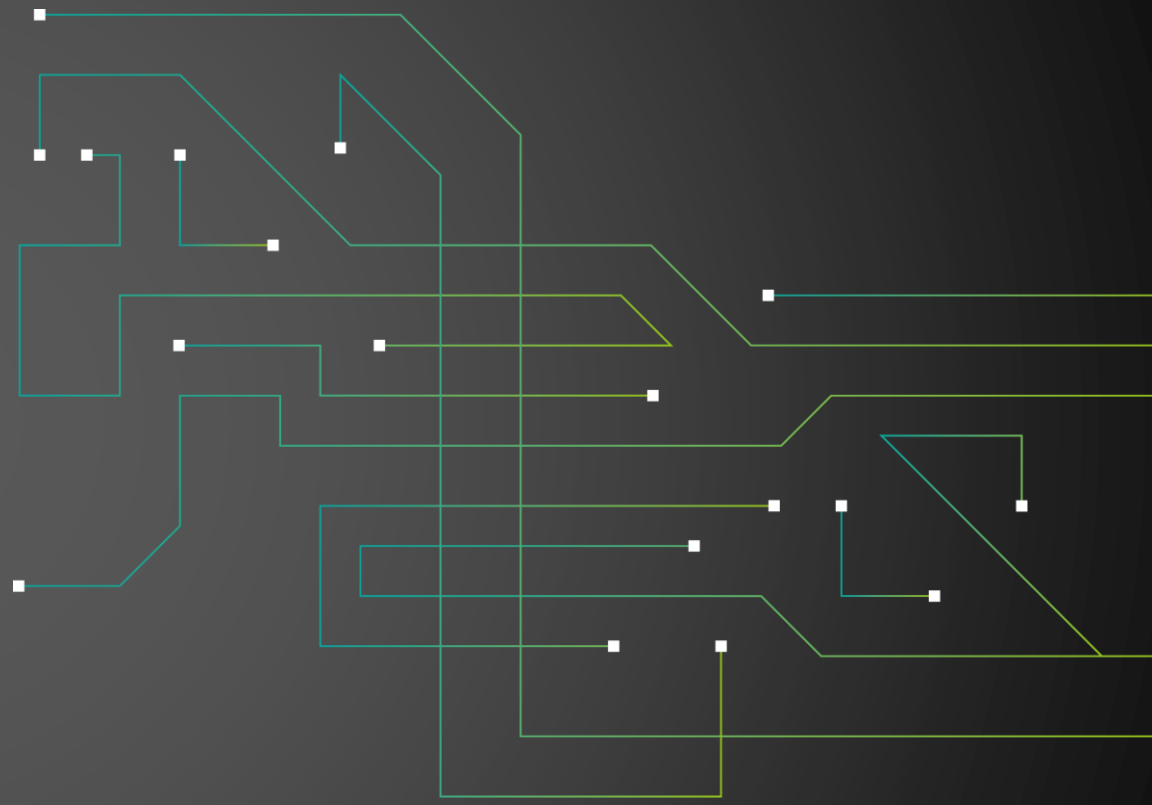
base it

WINDOWS 10>
SERVER 2019 >
MACOSX

WINDOWS 7 >
SERVER 2008R2 >

ANDROID
LINUX SERVER

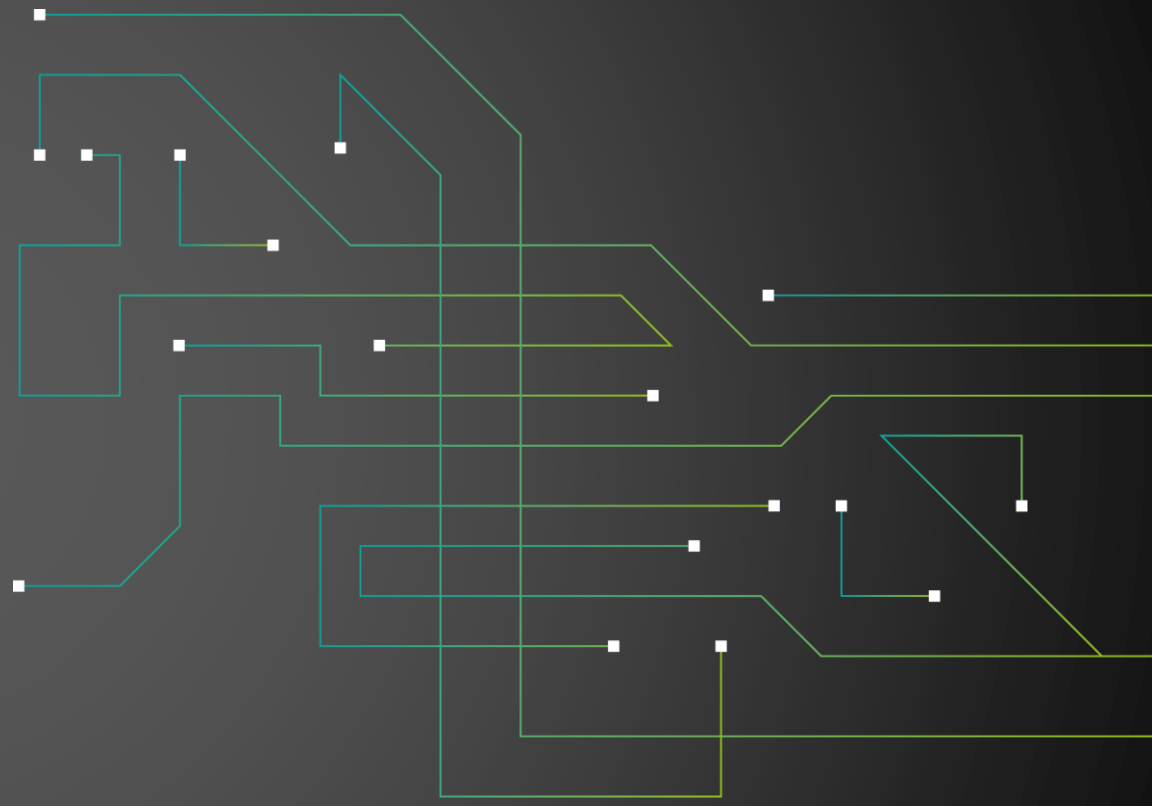
IOS



professional.
fast.
secure.

LIVE DEMO

base it



HTTPS://SECURITYCENTER.MICROSOFT.COM

professional.
fast.
secure.

WHATS NEW DEFENDER ATP

base it

CLIENTS

- LINUX ENTERPRISE SERVER
- ANDROID (DEVICE ADMIN & ANDROID FOR WORK)

EDR BLOCK MODE

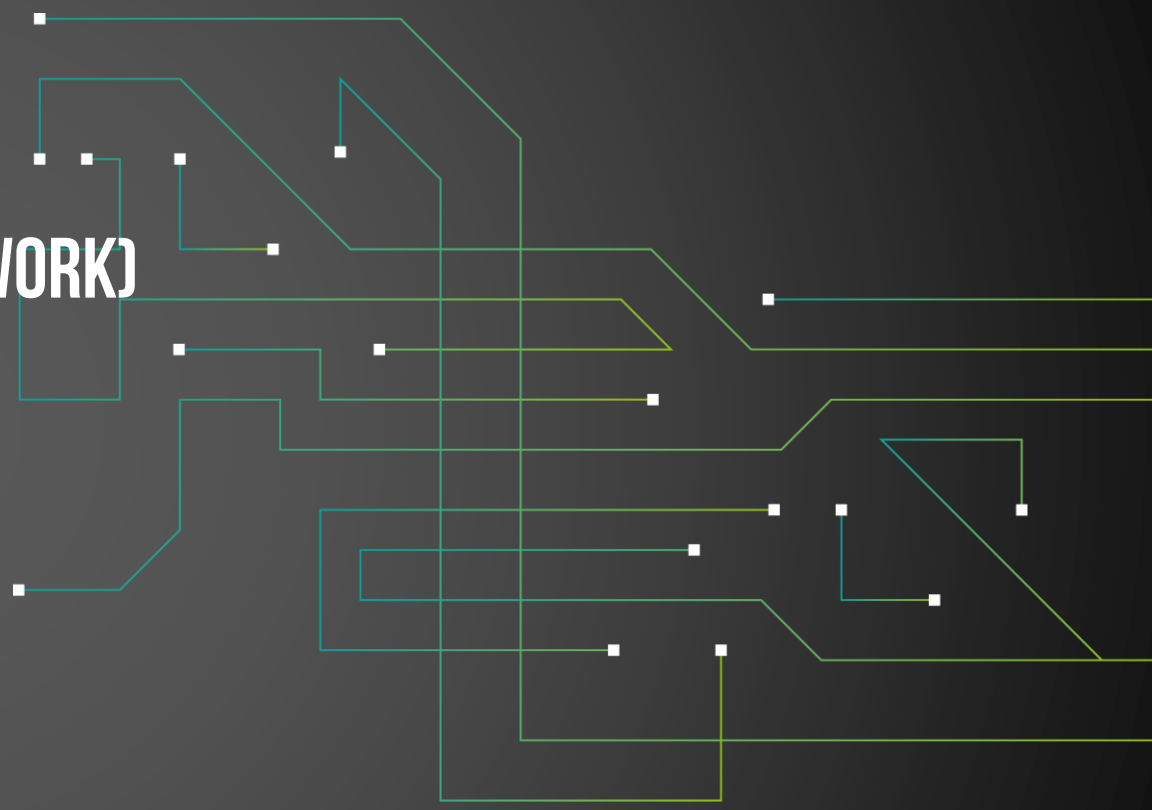
WEB CONTENT FILTERING (WITHOUT PARTNER)

UEFI SCANNER

VDI SUPPORT

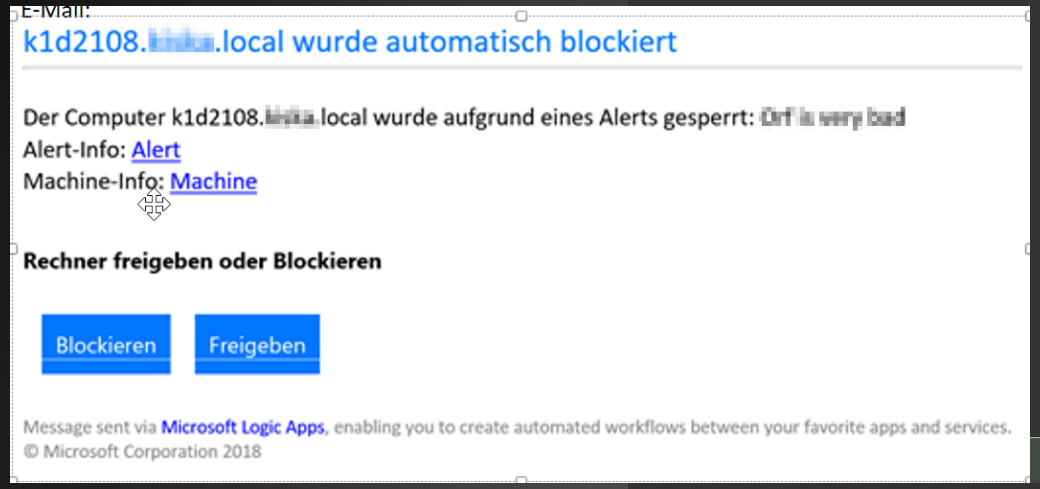
COVID-19 HARDENING

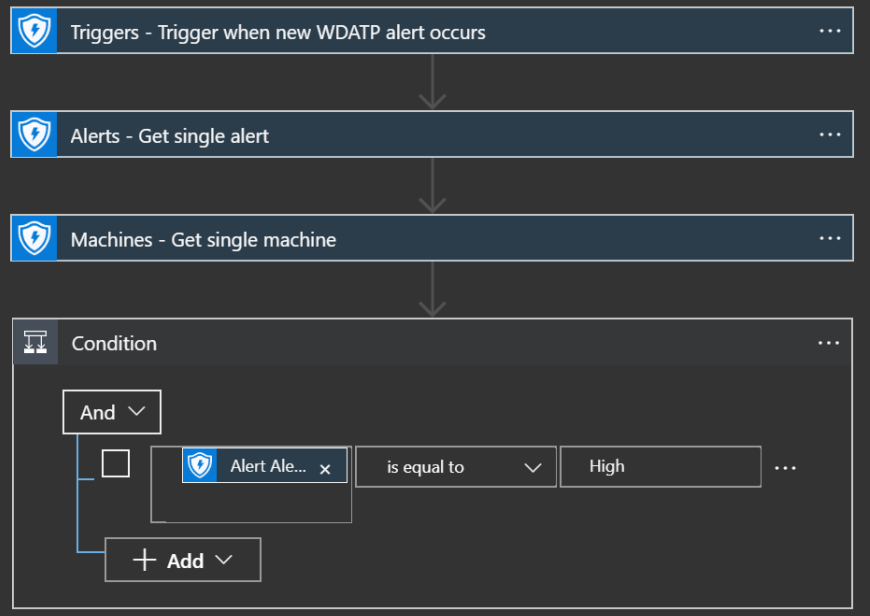
SECURE CONFIGURATION ASSESSMENT (SCA FOR SERVER)

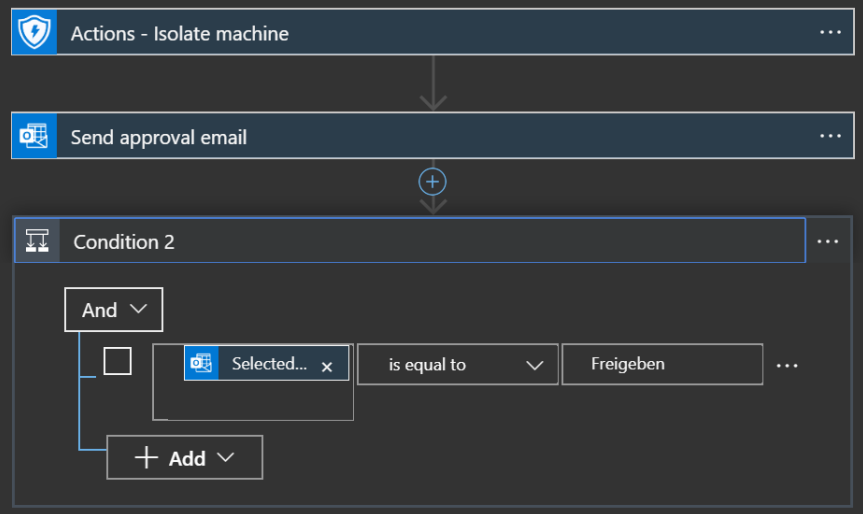


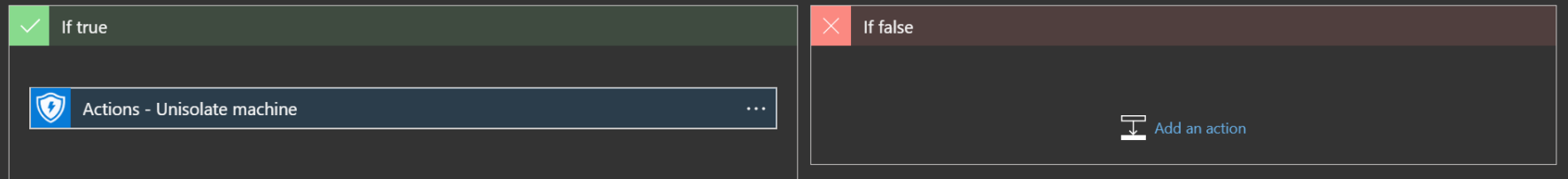
professional.
fast.
secure.

FEATURES

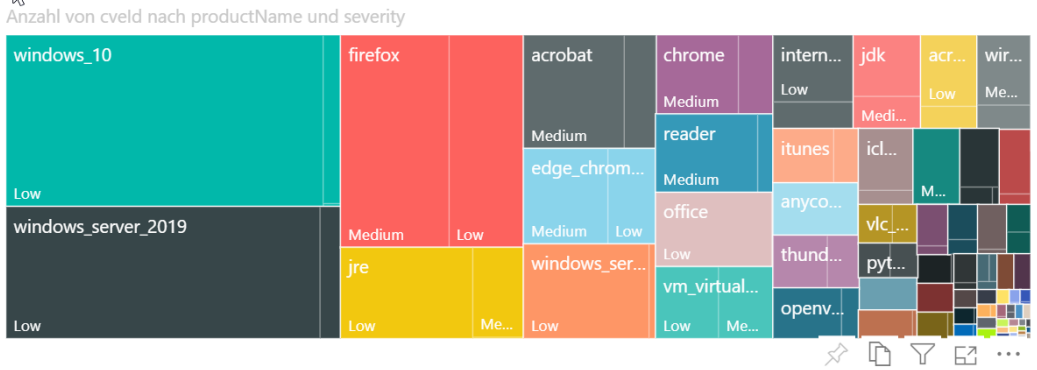

E-Mail:
k1d2108.[redacted].local wurde automatisch blockiert
Der Computer k1d2108.[redacted].local wurde aufgrund eines Alerts gesperrt: [redacted]
Alert-Info: Alert
Machine-Info: Machine
Rechner freigeben oder Blockieren
Blockieren
Freigeben
Message sent via Microsoft Logic Apps, enabling you to create automated workflows between your favorite apps and services.
© Microsoft Corporation 2018

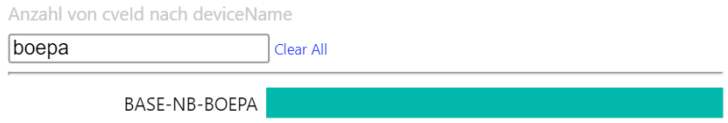

Triggers - Trigger when new WDATP alert occurs
Alerts - Get single alert
Machines - Get single machine
Condition
And
Alert Ale...
is equal to
High
Add


Actions - Isolate machine
Send approval email
Condition 2
And
Selected...
is equal to
Freigeben
Add


If true
Actions - Unisolate machine
If false
Add an action

FEATURES





cveId	deviceName	productName	productVendor	productVersion	severity
CVE-2018-20250	BASE-NB-HOLTH2	winrar	rarlab	5.1.0.0	High
CVE-2018-20250	BASE-NB-HUEMA	winrar	rarlab	5.50.0.0	High
CVE-2008-5353	BASE-NB-LEHPA	jre	oracle	1.4.2.0	High
CVE-2012-1723	BASE-NB-LEHPA	jre	oracle	1.4.2.0	High
CVE-2020-0646	BASE-NB-REICH2	.net_framework	microsoft	4.8.0.0	High
CVE-2018-20250	BASE-NB-SZEPE	winrar	rarlab	5.50.0.0	High
CVE-2018-20250	BASE-NB-TEUST	winrar	rarlab	5.61.0.0	High
CVE-2020-6556	BASE-NB-BAKMI	chrome	google	84.0.4147.125	Medium
CVE-2019-5589	BASE-NB-BAKMI	forticlient	fortinet	6.0.5.209	Medium
CVE-2019-16887	BASE-NB-BAKMI	irfanview	irfanview	4.53.0.0	Medium
CVE-2019-17241	BASE-NB-BAKMI	irfanview	irfanview	4.53.0.0	Medium
CVE-2019-17242	BASE-NB-BAKMI	irfanview	irfanview	4.53.0.0	Medium
CVE-2019-17243	BASE-NB-BAKMI	irfanview	irfanview	4.53.0.0	Medium
CVE-2019-17244	BASE-NB-BAKMI	irfanview	irfanview	4.53.0.0	Medium
CVE-2019-17245	BASE-NB-BAKMI	irfanview	irfanview	4.53.0.0	Medium
CVE-2019-17246	BASE-NB-BAKMI	irfanview	irfanview	4.53.0.0	Medium
CVE-2019-17247	BASE-NB-BAKMI	irfanview	irfanview	4.53.0.0	Medium
CVE-2019-17248	BASE-NB-BAKMI	irfanview	irfanview	4.53.0.0	Medium
CVE-2019-17249	BASE-NB-BAKMI	irfanview	irfanview	4.53.0.0	Medium
CVE-2019-17250	BASE-NB-BAKMI	irfanview	irfanview	4.53.0.0	Medium

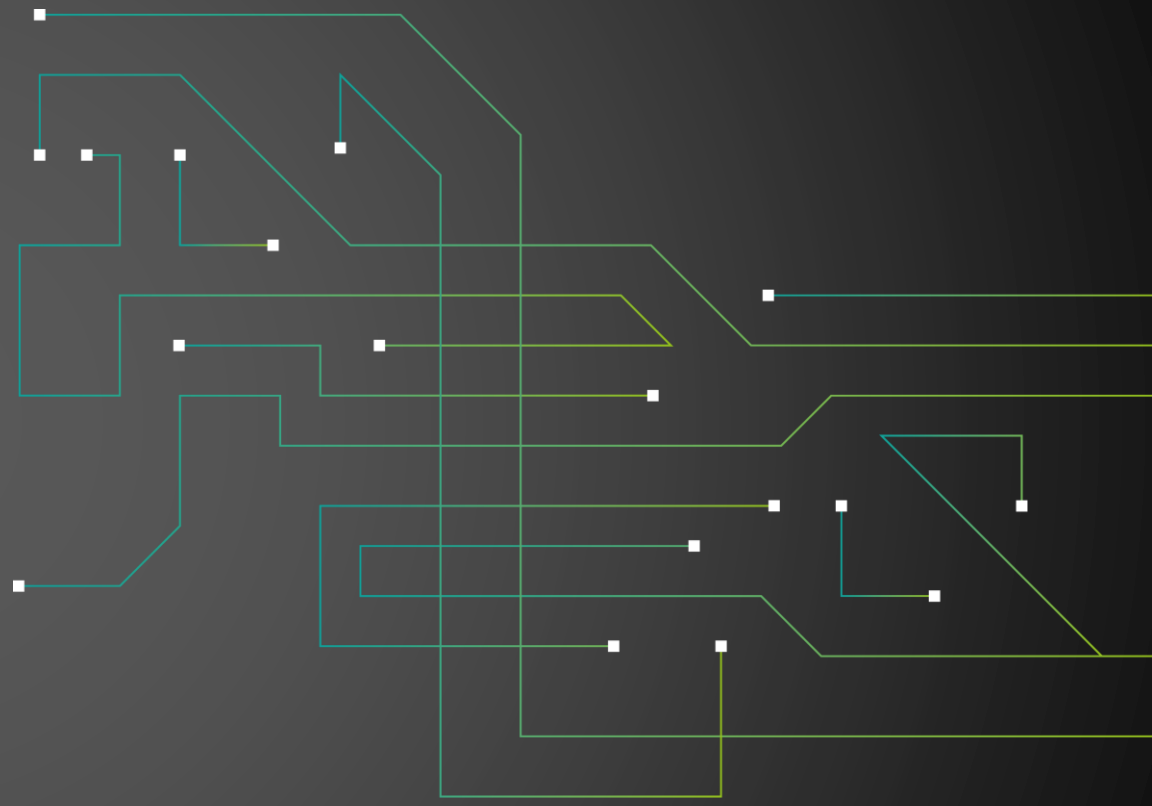
Hilfe anfordern

base it

professional.
fast.
secure.

THANK YOU

BASEIT.AT/WEBCAST



professional.
fast.
secure.