Cyber Security Roundtable Liechtenstein

Automatisierte Erkennung von
Cyber Angriffen mittels KI

malean

Michael Kürsteiner
Senior Manager
LC Systems

Sandra Thurnheer
Gründerin und Geschäftsführerin
malean

Cyber Security in der Praxis

Automatisierte Erkennung von Cyber Angriffen mittels KI

malean

LC SYSTEMS

THE DATA COMPANY

Vorstellung Vectra AI - Automatisierte Erkennung von Angriffssignalen mithilfe künstlicher Intelligenz (KI)

07. Februar 2024

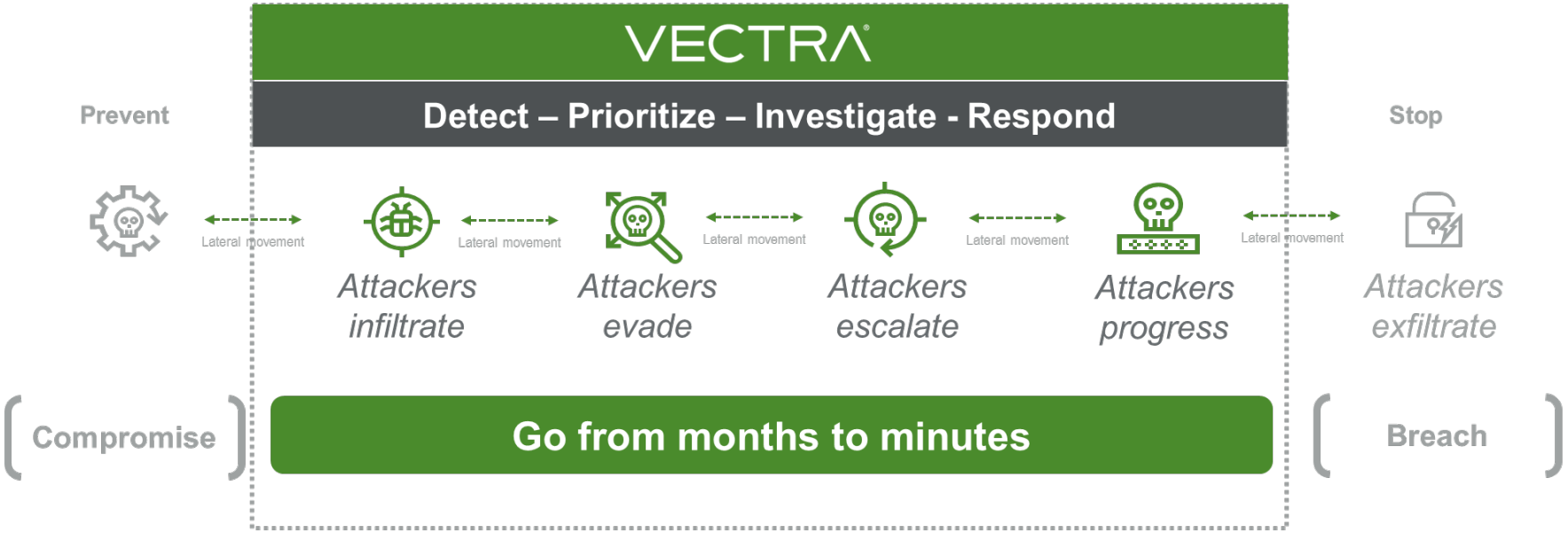
Warum braucht es KI in der IT-Security?

- More Remote Users
- More Cloud Services
- More Cloud Vulnerabilities
- More Account Compromise
- More Network Devices
- More Lateral Movement

Spiral of MORE

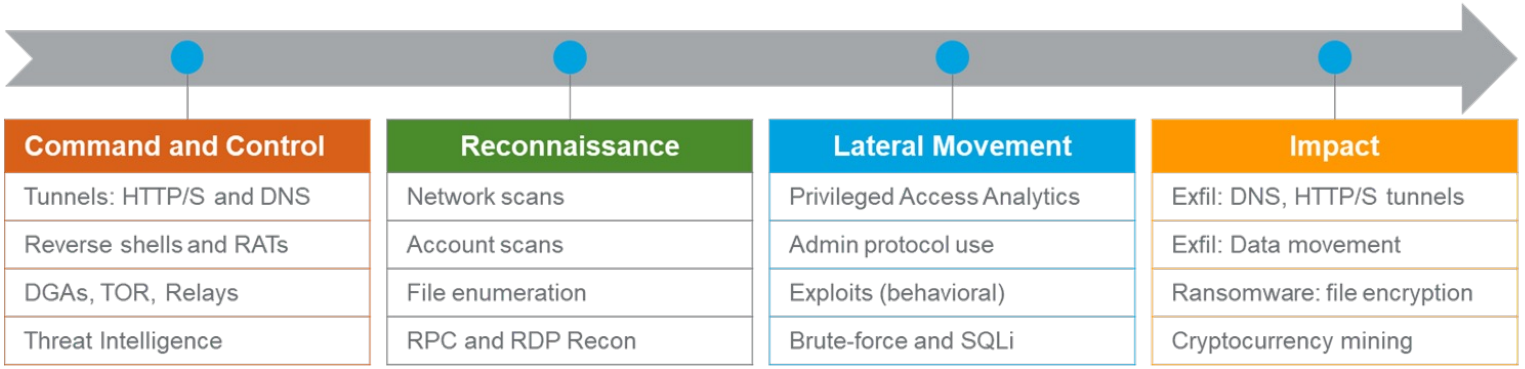
- More Attack Surface
- More Evasive Attackers
- More Blind Spots
- More Attacker Exploits
- More Alert Triage
- More Analyst Workload

Vectra verwendet KI, damit Sie sich mit der Geschwindigkeit der Angreifer bewegen können



Methodiken & Tools der Bedrohungsakteure

- Threat actors have 1000's of tools and tactics, but behaves similarly
  1. They establish a control mechanism into the compromised environment (C2)
  2. They snoop around to map out the compromised environment (Recon)
  3. They move laterally inside the compromised environment (Lateral movement)
  4. They steal, encrypt, alter and destroy (Impact)



Command and Control	Reconnaissance	Lateral Movement	Impact
Tunnels: HTTP/S and DNS	Network scans	Privileged Access Analytics	Exfil: DNS, HTTP/S tunnels
Reverse shells and RATs	Account scans	Admin protocol use	Exfil: Data movement
DGAs, TOR, Relays	File enumeration	Exploits (behavioral)	Ransomware: file encryption
Threat Intelligence	RPC and RDP Recon	Brute-force and SQLi	Cryptocurrency mining

Erkennung von Angreifer-Methoden

1

Analyze
attacker methods

MITRE | ATT&CK®

Per-domain analysis
enables deep coverage

2

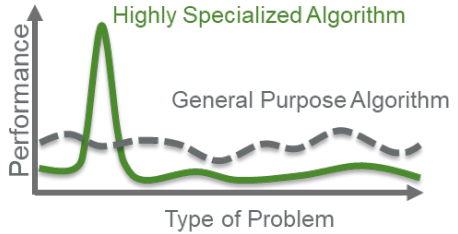
Define
countermeasures

MITRE | D3FEND™

Define techniques to
detect attack methods

3

Use the **optimal ML**
approach for each



Security-led approach to AI

Powered by cutting-edge ML

Outcome: more coverage and clarity, less noise
vs simple anomaly-based detection

Angriffssignale zu finden ist in Vectras DNA

35 Patents
150+ models spanning neural networks, unsupervised, novelty

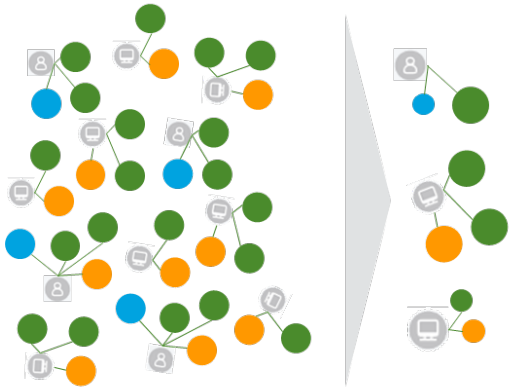
12 MITRE References
Most patent references of any security vendor

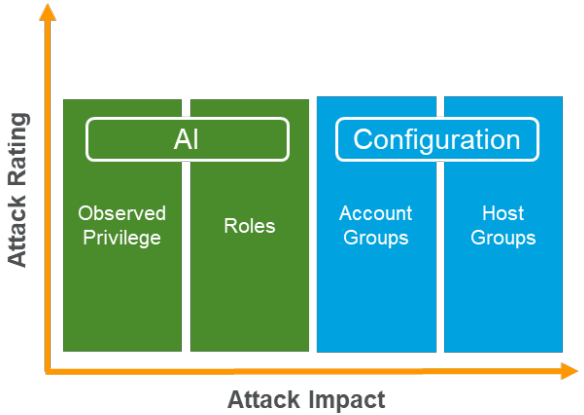
Network Effect
Continuous feedback from 1,000+ customers

AI-driven Attack Signal Intelligence™

Vectra KI-gesteuerte Attack Signal Intelligence™

Think like an attacker	Know what is malicious & important	Focus on what is urgent
AI-driven Detections	AI-driven Triage	AI-driven Prioritization





Vectra Attack Signal Intelligence™

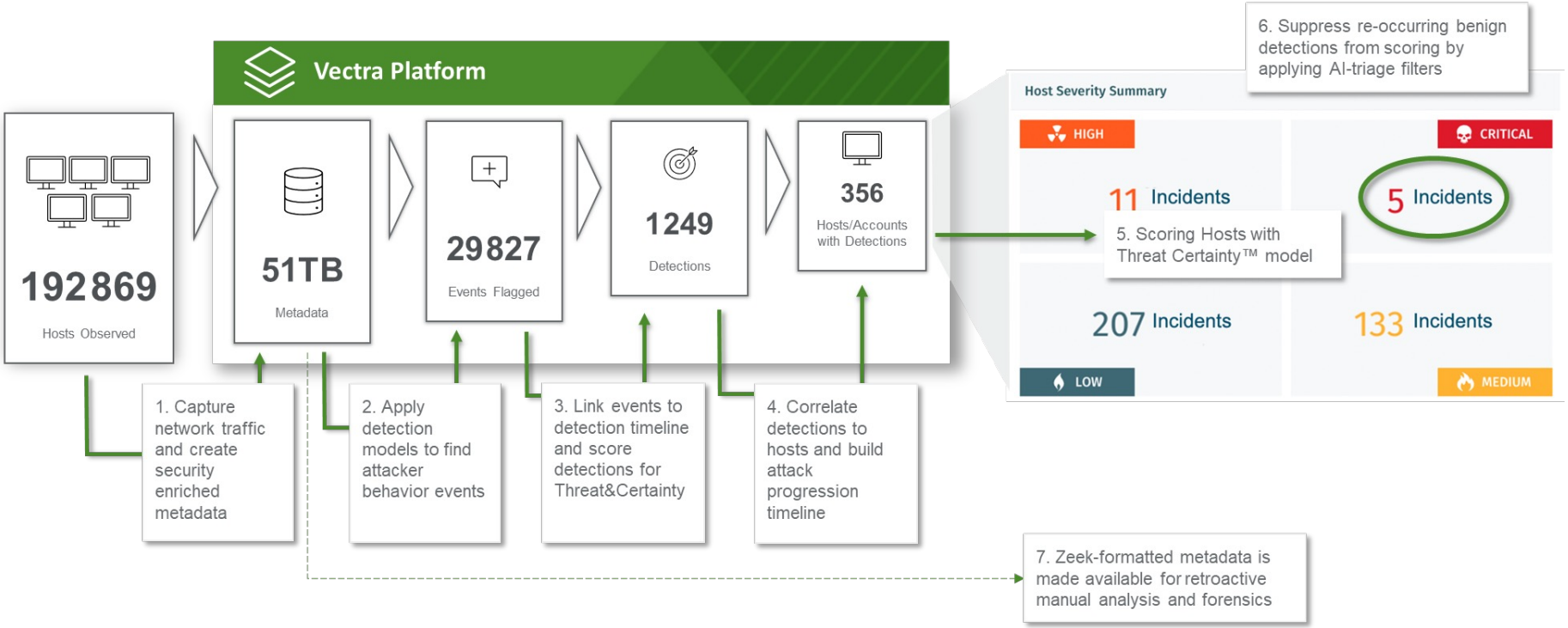
LC SYSTEMS

Attack Progression

Access	Persist	Command & Control	Escalate & Evade	Recon & Discover	Lateral Movement	Exfiltration & Disruption
New Host	MFA Disabled	Hidden HTTPS Tunnel	New Host Role	Kerberoasting (x2)	Privilege Access Anomaly (x6)	Smash and Grab
Suspected Compromise Access	Trusted IP Change	Hidden DNS Tunnel	Log Disabling Attempt	Internal Darknet Scan	Suspicious Remote Exec	Ransomware File Activity
Brute-Force Attempt/Success	Admin Account Creation	Hidden HTTP Tunnel	Disabling Security Tools	Port Scan	Suspicious Remote Desktop	Data Gathering
Disabled Account	Account Manipulation	Multi-homed Fronted Tunnel	Suspicious Mailbox Rule	Port Sweep	Suspicious Admin	Data Smuggler
TOR Activity	Redundant Access	Suspicious Relay	Log Disabling Attempt	SMB Account Scan	Shell Knocker	Hidden DNS Tunnel Exfil
Unusual Scripting Engine	Logging Disabled	Suspect Domain Activity	Suspect Privilege Escalation	Kerberos Account Scan	Automated Replication	Hidden HTTP/S Tunnel Exfil
Suspicious OAuth App	User Hijacking	Malware Update	Suspect Privilege Manipulate	Kerberos Brute-Sweep	Brute-Force	Botnet Abuse Behaviors
Suspicious Sign-On	ECS Hijacking	Peer-to-Peer	Suspect Console Pivot	File Share Enumeration	SMB Brute-Force	Crypto mining
Suspicious Sign-On with MFA Fail	Suspect Login Profile Manipulation	Suspicious HTTP	Suspect Cred Access EC2	Suspicious LDAP Query	Kerberos Brute Force	External Teams Access
Suspicious Teams App	Security Tools Disabled	Stealth HTTP Post	Suspect Cred Access SSM	RDP Recon	SQL Injection Activity	Ransomware SharePoint Activity
Suspicious Credential Usage	SSM Hijacking	TOR Activity	Suspect Cred Access ECS	RPC Recon	Internal Stage Loader	Suspicious SharePoint Download
Root Credential Usage		Novel External Port	Suspect Cred Access Lambda	RPC Targeted Recon	Suspicious Active Directory	Suspicious SharePoint Sharing
TOR Activity		Threat Intel Match		Unusual eDiscovery Search	Novel Admin Protocol	Exfil Before Termination
		Vectra Threat Intel Match		Unusual Compliance Search	Novel Admin Share Access	Suspicious Mailbox Forwarding
				Suspect eDiscovery Activity	Risky Exchange Op	eDiscovery Exfil
				User Permission Enumeration	Internal Spear phishing	Power Automate Activity (x3)
				EC2 Enumeration	File Poisoning	Ransomware S3 Activity
				S3 Enumeration	Mailbox Manipulation	Suspect Public S3 Change
				Suspect Escalation Recon	DLL Hijacking	Suspect Public EBS Change
				Organization Discovery	Privilege Operation Anomaly	Suspect Public EC2 Change
						Suspect Public RDS Change
						Suspect External Access Grant

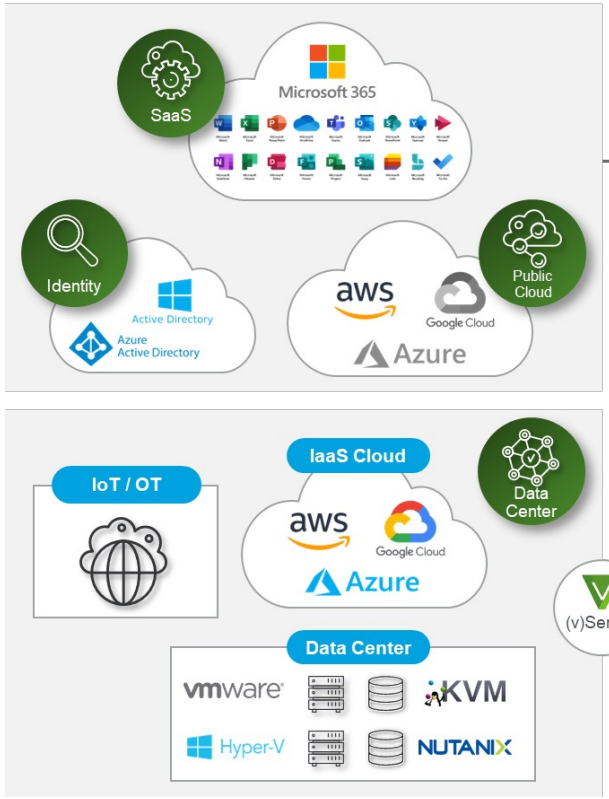
- Hybrid Network and Identity
- Identity: Azure AD
- Public Cloud: AWS
- SaaS: Microsoft 365

Unübertroffene Signal-Klarheit durch intelligente Automatisierung & Priorisierung



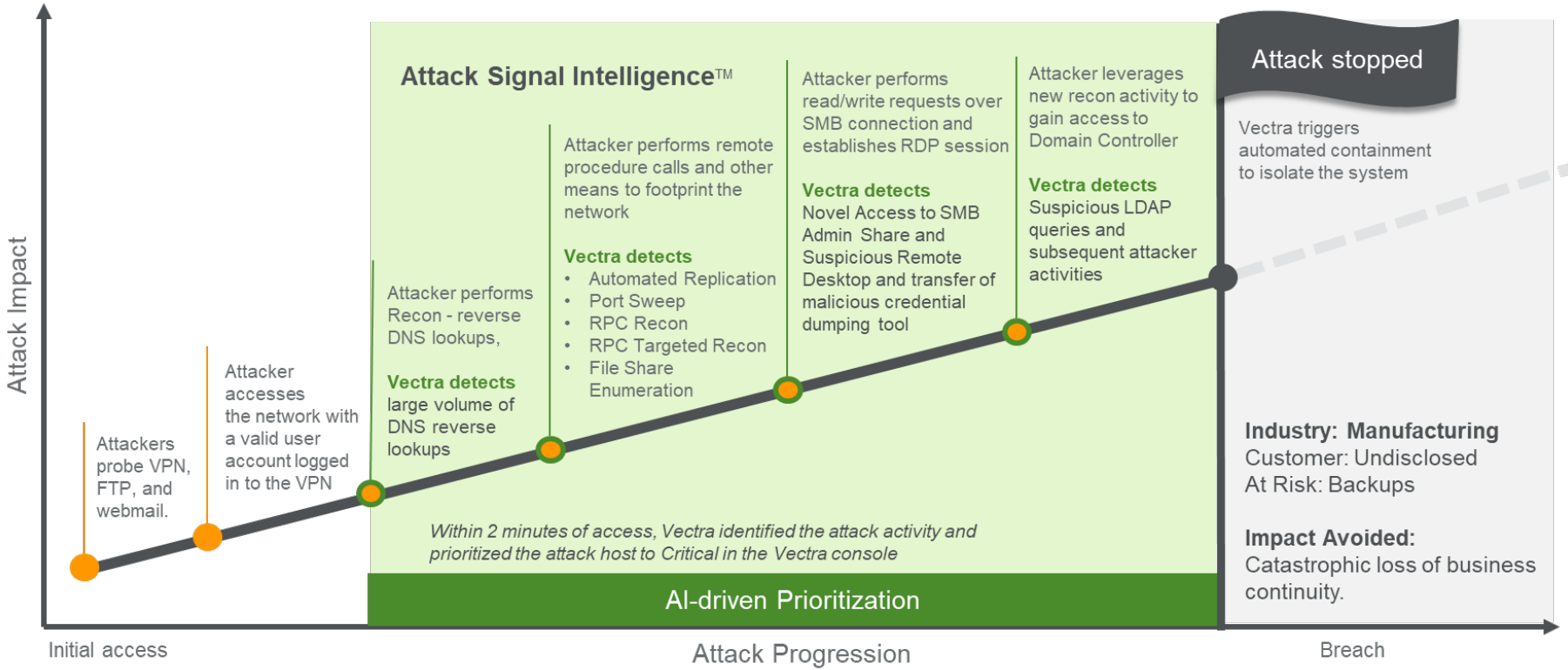
Source: Customer environment in a large multinational enterprise, during a 30 day period

Vectra Hybrid-Cloud Plattform-Architektur



- Native coverage
- Integrate any EDR
- Real-time detections
- Enterprise scale
- Intuitive SaaS UX
- Modular design
- Agentless
- Ecosystem-friendly
- 24x7x365 MDR services

Realer Vorfall: Angriffsignale durch RansomOps



LC SYSTEMS

THE DATA COMPANY

Vielen Dank für Ihre Aufmerksamkeit.