CORTEX
BY PALO ALTO NETWORKS

How Cortex can help Healthcare organisations?

paloalto NETWORKS

Palo Alto Networks Portfolio

Strata PA-Series
ML-Powered Next-Generation Firewall
App-ID | User-ID | Content-ID | Device-ID

VM-Series
Virtual Next-Generation Firewall
App-ID | User-ID | Content-ID | Device-ID

CN-Series
Containerized Next-Generation Firewall
App-ID | User-ID | Content-ID | Device-ID

Panorama
Firewall Management

Prisma Access
Secure Access Service Edge
FWaaS | Secure Web Gateway | Zero Trust Network Access

Prisma Cloud
Cloud Native Security Platform
Cloud Security Posture Management | Cloud Workload Protection | Cloud Network Security | Cloud Infrastructure Entitlement Management

Prisma SD-WAN
Next-Generation SD-WAN
SD-WAN

Cortex XDR
Extended Detection and Response
Endpoint Threat Prevention | Endpoint Detection & Response | Behavioral Analytics | Managed Detection & Response

Cortex XSOAR
Extended Security Orchestration, Automation and Response
Security Orchestration, Automation & Response | Threat Intelligence Management

Expanse
Attack Surface Management
Internet-Connected Asset Discovery & Mitigation

Unit42
Cybersecurity Services
Data Breach Response | Cyber Risk & Resilience Management | Incident Response Services

Cloud-Delivered Security Services

DNS Security	Threat Prevention	URL Filtering	WildFire	IoT Security	GlobalProtect	SD-WAN	Data Loss Prevention	Prisma SaaS
DNS Attack Prevention	Exploit, Malware, C2 Prevention	Malicious Site & Phishing Prevention	Malware Prevention	Enterprise IoT Security	Mobile User Security	Secure Branch Connectivity	Data Protection & Compliance	In-line & API SaaS Application Security

paloalto NETWORKS

Healthcare security challenges :

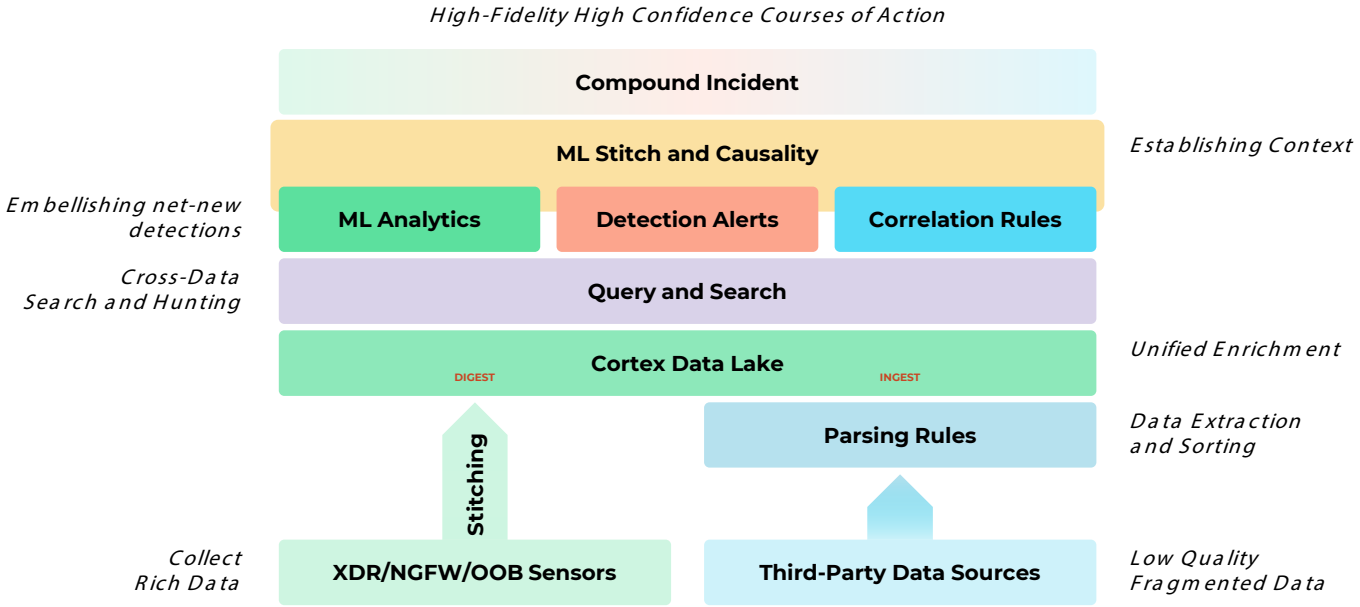
- Budget constraints
- Lack of security personnel
- Difficulty to apply consistent security policies across all the departments (Flexibility / local management, shadow IT, Heterogeneous IT & unmanaged assets)
- Sophisticated attacks are targeting significantly healthcare organisations, impacting the CIA of the patient data

How Cortex might help? : Budget constraint

Conceptual view

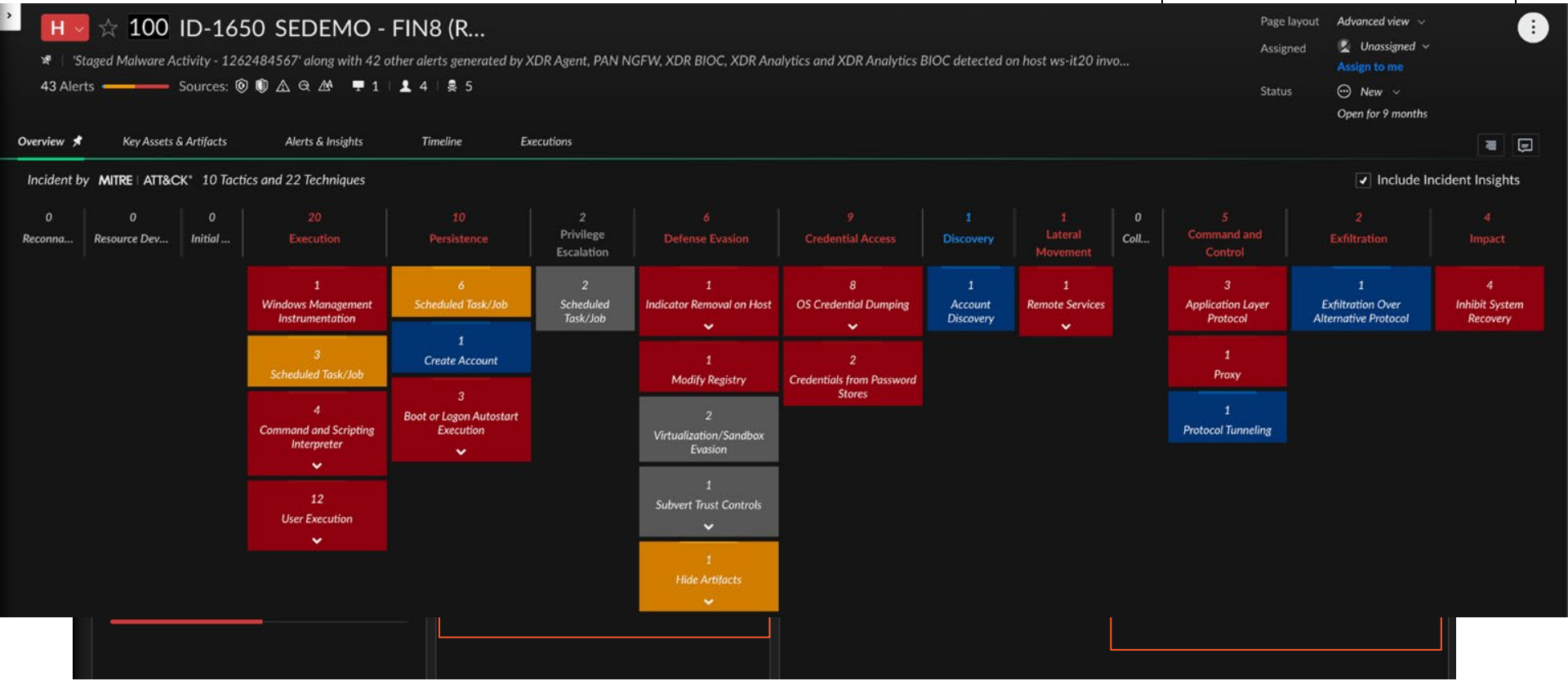
Cortex solution : **CONSOLIDATION and CENTRALIZATION of security objects**

You cannot secure what you cannot see…



How Cortex might help? : Budget constraint

Technical view

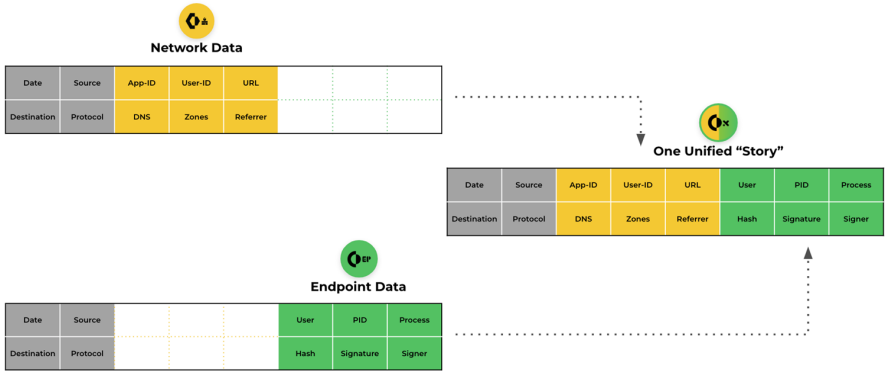


How Cortex might help? : Lack of security personnel

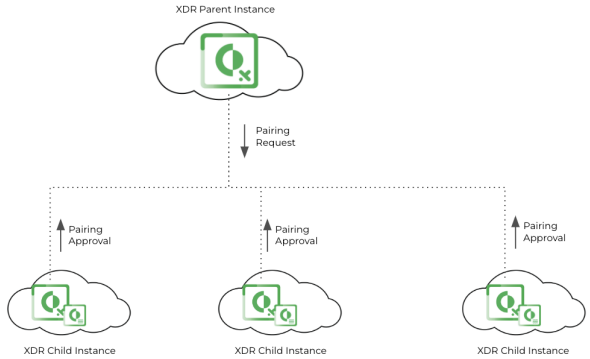
Conceptual view

Cortex solution : **Stitching of data (NGFW, O365, Cloud, etc...) / Multi-tenancy support**

Data normalization and smart incident generation



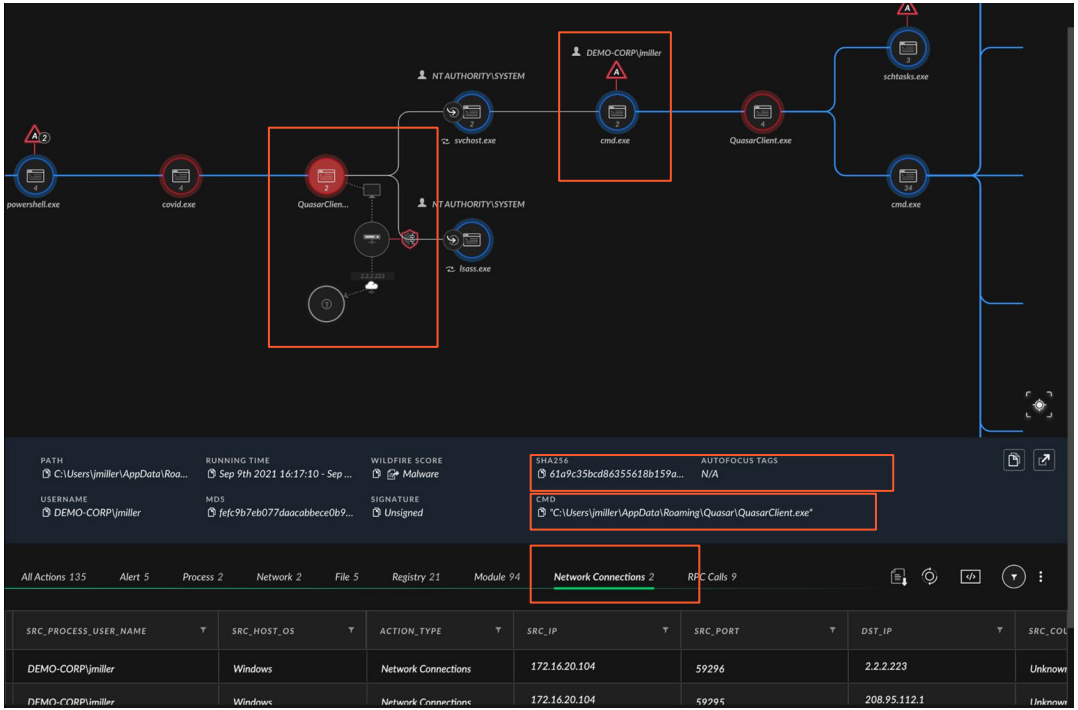
Data is key (Visualisation / Analytics / Automation)



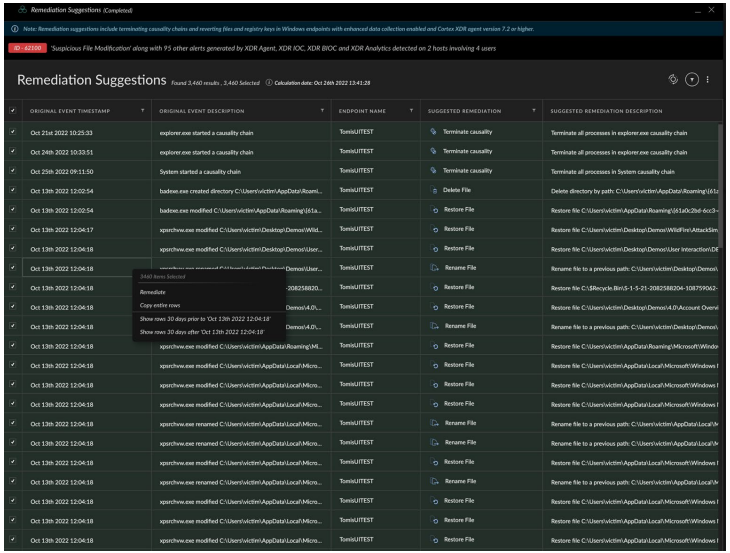
-State of the art technology for Multi-tenancy Share responsibility model
-Advanced service (Assessment, MSS, Threat hunting, Incident response/retainer)

How Cortex might help? : Lack of security personnel

Technical view



Full incident story to pivot from ...



Remediation suggestion, baseline for automated actions

How Cortex might help? : Security policy consistency

Conceptual view

Cortex solution : **Single platform for deployment, asset discovery, extended tooling**

Single platform for Server, Mobile, Win/Mac end user

Discover

- Agent discovery
- Local mapping (Broker VM)
- AD import
- Cloud import
- Analytics

Install

- Package deployment with local tools
- Lightweight agent
- Log collection only
- Dynamic group policy
- Unified agent (cloud/local)

Manage

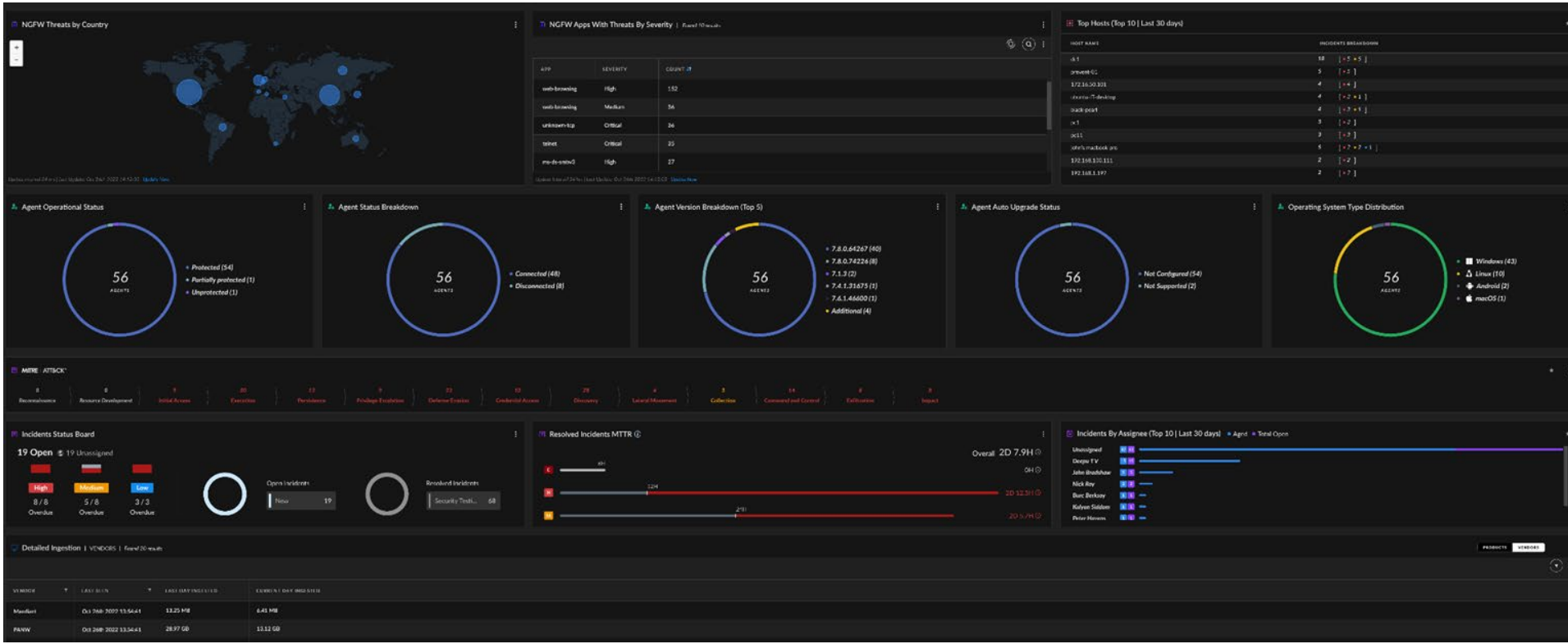
- Local/Global exceptions (incl.Hardening)
- Agent Auto-Update with test environment
- Automate IoC/changes from API (Automation services)

Improve

- Customize local detection
- Report on incident closure
- Measure your MTTD/R
- SOC tool improvement (qualitative log sources, vendor support,etc..)

How Cortex might help? : Security policy consistency

Technical view



 |

How Cortex might help? : Sophisticated attacks

Conceptual view

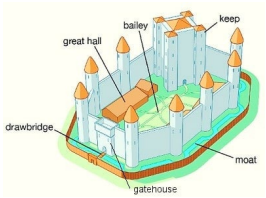
Cortex solution : **State of the art prevention, detection, analytics and response technology**

Complete protection lifecycle

HARDENING

- Device control
- Check Encrypt
- Host Firewall

PREVENTION



- Exploit prevention (Technique + Netw. based)
- Malware prevention (ML / Sandbox)
- Malicious Behaviour prevention

ADV. DETECTION

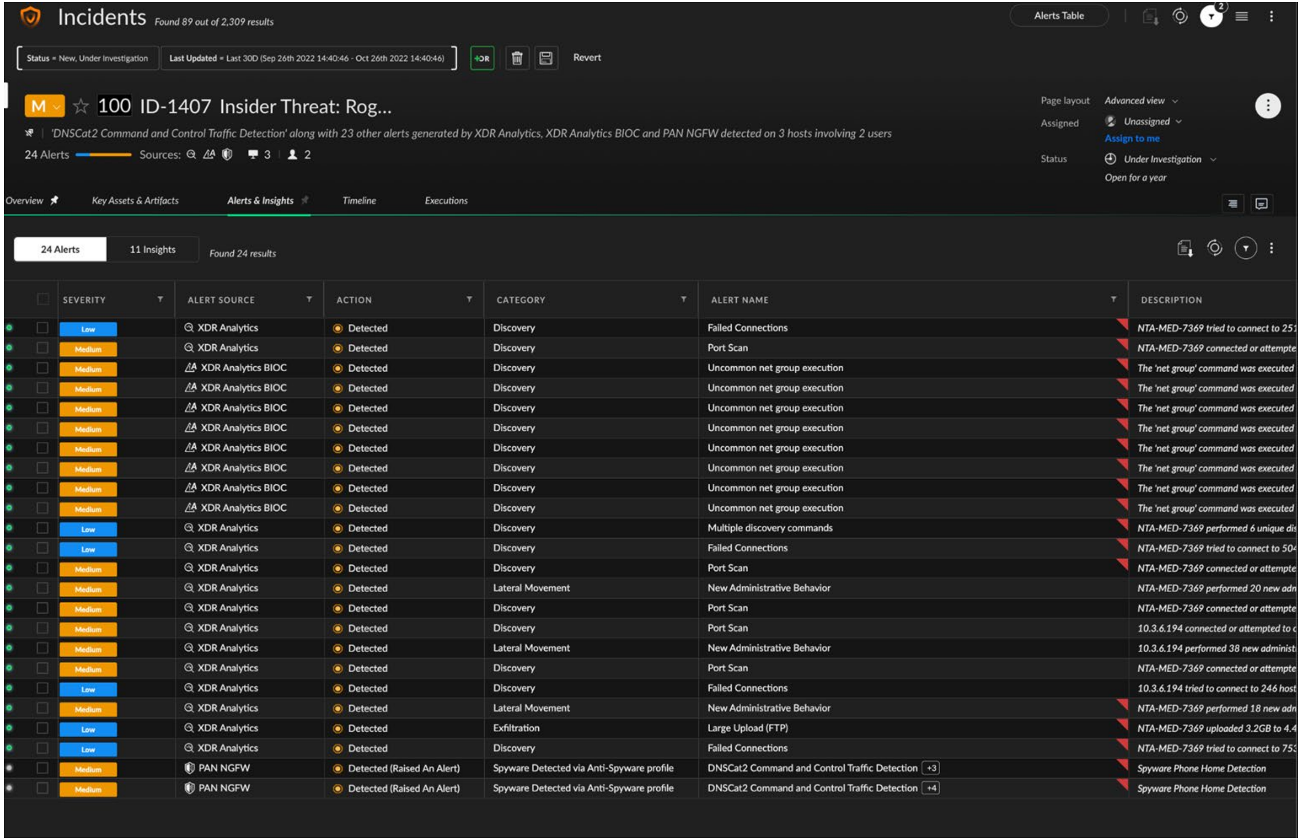
- Telemetry based detection
- Analytics based detection
- Correlation based detection

RESPONSE

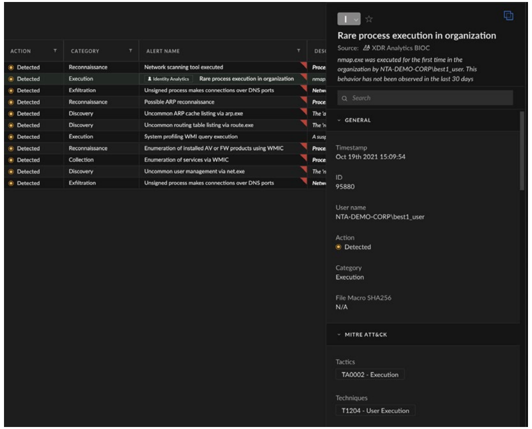
- Full remote access
- Python script execution
- Powerful query language
- Forensics module

How Cortex might help? : Sophisticated attacks

Technical view



SEVERITY	ALERT SOURCE	ACTION	CATEGORY	ALERT NAME	DESCRIPTION
Low	XDR Analytics	Detected	Discovery	Failed Connections	NTA-MED-7369 tried to connect to 251
Medium	XDR Analytics	Detected	Discovery	Port Scan	NTA-MED-7369 connected or attempte
Medium	XDR Analytics BIOC	Detected	Discovery	Uncommon net group execution	The 'net group' command was executed
Medium	XDR Analytics BIOC	Detected	Discovery	Uncommon net group execution	The 'net group' command was executed
Medium	XDR Analytics BIOC	Detected	Discovery	Uncommon net group execution	The 'net group' command was executed
Medium	XDR Analytics BIOC	Detected	Discovery	Uncommon net group execution	The 'net group' command was executed
Medium	XDR Analytics BIOC	Detected	Discovery	Uncommon net group execution	The 'net group' command was executed
Medium	XDR Analytics BIOC	Detected	Discovery	Uncommon net group execution	The 'net group' command was executed
Medium	XDR Analytics BIOC	Detected	Discovery	Uncommon net group execution	The 'net group' command was executed
Medium	XDR Analytics BIOC	Detected	Discovery	Uncommon net group execution	The 'net group' command was executed
Low	XDR Analytics	Detected	Discovery	Multiple discovery commands	NTA-MED-7369 performed 6 unique dis
Low	XDR Analytics	Detected	Discovery	Failed Connections	NTA-MED-7369 tried to connect to 504
Medium	XDR Analytics	Detected	Discovery	Port Scan	NTA-MED-7369 connected or attempte
Medium	XDR Analytics	Detected	Lateral Movement	New Administrative Behavior	NTA-MED-7369 performed 20 new adn
Medium	XDR Analytics	Detected	Discovery	Port Scan	NTA-MED-7369 connected or attempte
Medium	XDR Analytics	Detected	Discovery	Port Scan	10.3.6.194 connected or attempted to c
Medium	XDR Analytics	Detected	Lateral Movement	New Administrative Behavior	10.3.6.194 performed 38 new administ
Medium	XDR Analytics	Detected	Discovery	Port Scan	NTA-MED-7369 connected or attempte
Low	XDR Analytics	Detected	Discovery	Failed Connections	10.3.6.194 tried to connect to 246 host
Medium	XDR Analytics	Detected	Lateral Movement	New Administrative Behavior	NTA-MED-7369 performed 18 new adn
Low	XDR Analytics	Detected	Exfiltration	Large Upload (FTP)	NTA-MED-7369 uploaded 3.2GB to 4.4
Low	XDR Analytics	Detected	Discovery	Failed Connections	NTA-MED-7369 tried to connect to 753
Medium	PAN NGFW	Detected (Raised An Alert)	Spyware Detected via Anti-Spyware profile	DNSCat2 Command and Control Traffic Detection +3	Spyware Phone Home Detection
Medium	PAN NGFW	Detected (Raised An Alert)	Spyware Detected via Anti-Spyware profile	DNSCat2 Command and Control Traffic Detection +4	Spyware Phone Home Detection



 |

THANK YOU