Validating Your Defenses with MITRE ATT&CK

How to test your security with Cortex XDR and SafeBreach, using MITRE ATT&CK

Agenda

MITRE ATT&CK Framework & Evaluations

ATT&CK Round 4 Results

SafeBreach and Cortex Integration

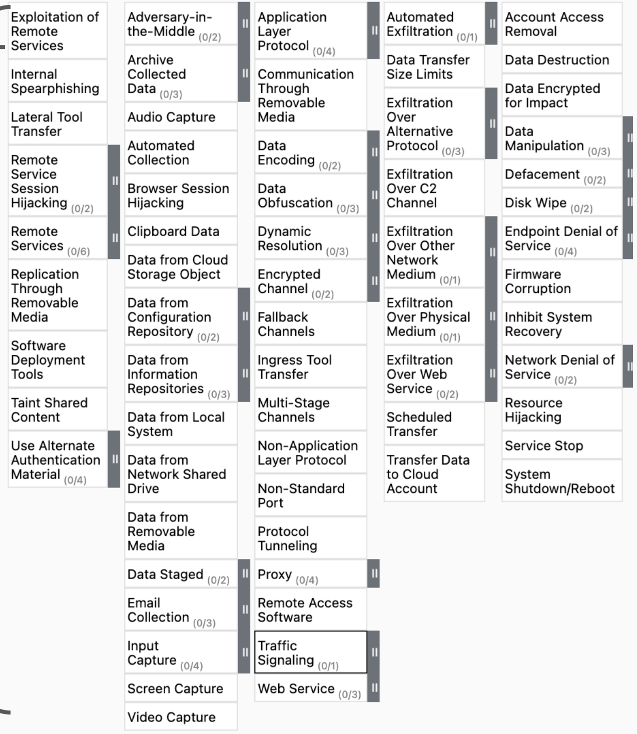
Q&A

About the MITRE ATT&CK Framework & Evaluations

The MITRE ATT&CK Framework

- The **MITRE ATT&CK Framework** has become **the standard** for how the security world communicates about adversaries and their techniques
- **ATT&CK** stands for Adversarial Tactics, Techniques & Common Knowledge

MITRE Enterprise ATT&CK Framework



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
									Exploitation of Remote Services	Adversary-in-the-Middle (0/2)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
									Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
									Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
									Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
									Remote Services (0/6)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
									Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
									Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
									Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
									Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
										Data from Local System	Non-Application Layer Protocol		Network Denial of Service (0/2)
										Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
										Data from Removable Media	Protocol Tunneling		Service Stop
										Data Staged (0/2)	Proxy (0/4)		System Shutdown/Reboot
										Email Collection (0/3)	Remote Access Software		
										Input Capture (0/4)	Traffic Signaling (0/1)		
										Screen Capture	Web Service (0/3)		
										Video Capture			

Adversaries Tactics

- What are they doing?
- Why are they doing it?

Adversaries Techniques

- How are they doing it?

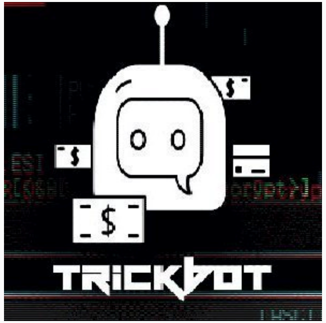
MITRE Engenuity ATT&CK Evaluations

- **Motivation behind the ATT&CK Evaluations?**
  - "Vendors are using ATT&CK to articulate their capabilities, but there is no neutral authority to evaluate their claims"
- **What ARE the ATT&CK Evaluations?**
  - Open, transparent & objective. Methodology and results published openly and clearly
  - Evaluates both Protection and Detection efficacy (Protection starting round 3)
  - Simply a compilation of the detections MITRE Engenuity observes in response to an emulated adversary's tactics and techniques
- **What are they NOT?**
  - Not designed to address noise or false positives
  - Not meant to be a competitive analysis that produces a score
  - No rankings or ratings

Enterprise 4 Evaluations

Wizard Spider & Sandworm

Enterprise 4 Adversaries: Wizard Spider



- Russia-based - Financially motivated
- Also Known As:
  - MITRE ATT&CK Group ID: G0008
  - Grim Spider, UNC1878, TEMP.MixMaster

- Known For:
  - Conti ransomware
  - TrickBot
  - Ryuk Ransomware
  - CISA Alert: Ransomware campaign against US Hospitals
  - Linked to Russia through TrickBot Leaks

A Closer Look at Conti Ransomware Used by Wizard Spider

144% ⬆

AVERAGE DEMAND IN 2021

78% ⬆

AVERAGE PAYMENT IN 2021

2022 Unit 42 Ransomware Threat Report

Understand trends and tactics to bolster defenses.

Figure 11: Sectors and industries most heavily targeted by ransomware (leak site data)

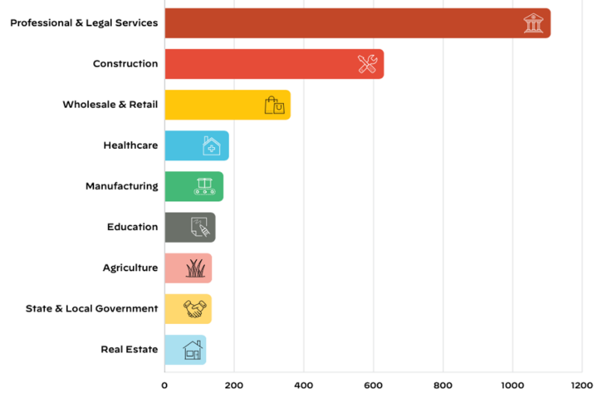
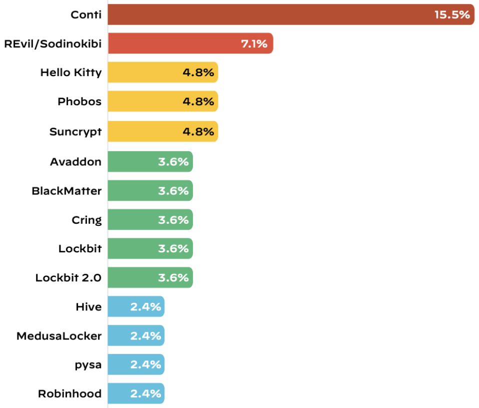


Figure 4: Most active ransomware variant in 2021 – Unit 42 incident response data



Conti stands out as one of the most ruthless ransomware gangs since their emergence in 2020.

$118,114

2020 INITIAL (ONLY OBSERVED) RANSOM DEMAND

$50K

MARCH 2021 INITIAL RANSOM DEMAND

$1.78M

AVERAGE 2021 RANSOM DEMAND

$3M

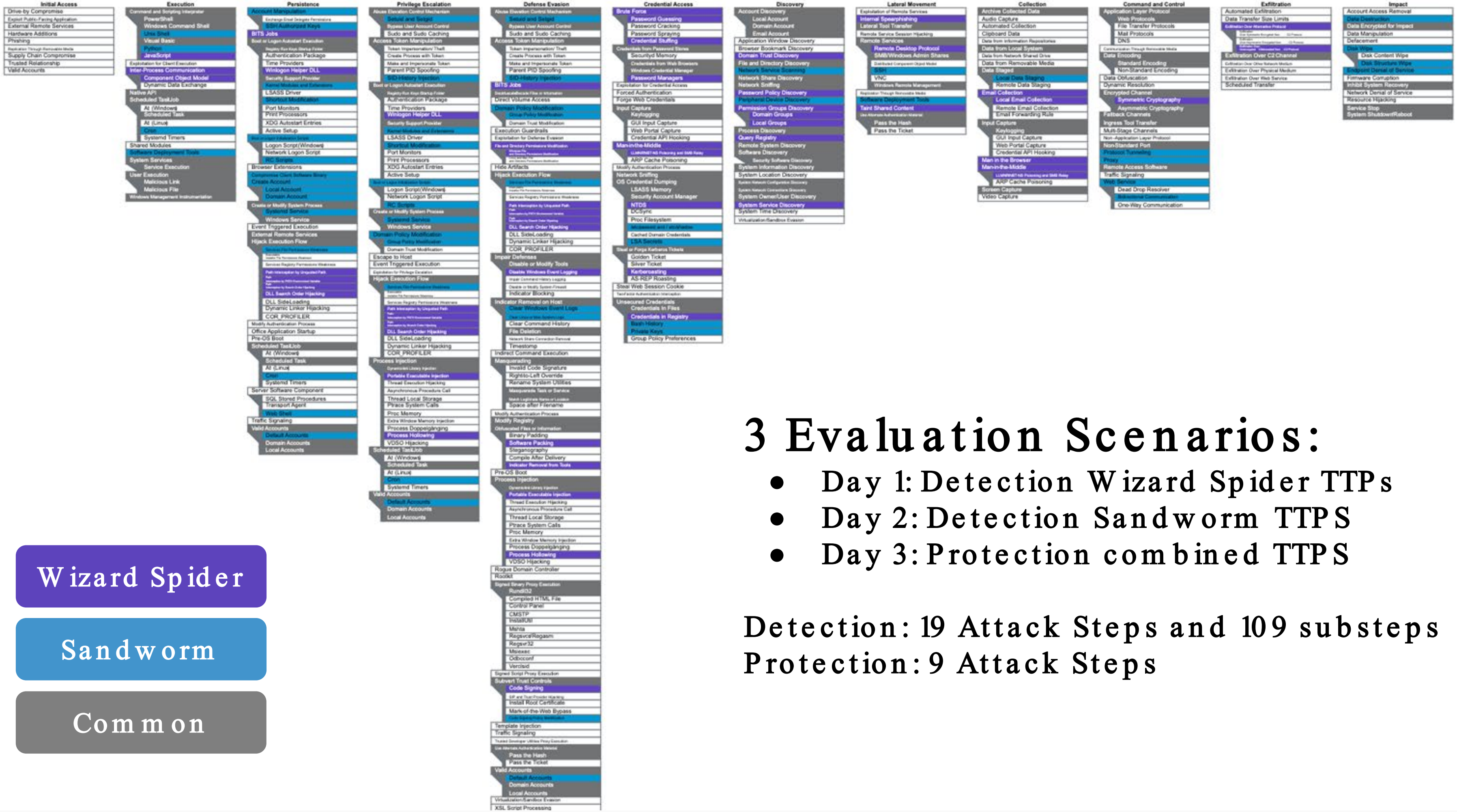
TOP 2021 REQUEST

Enterprise 4 Adversaries: Sandworm

- Russia-based destructive threat group
- Also Known As:
  - ATT&CK Group ID: G0034
  - Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455.
  - ELECTRUM, Telebots, IRON VIKING, BlackEnergy, Quedagh, VOODOO BEAR

- Known For:
  - 2015-2016 Attacks against Ukrainian Electrical Infrastructure

  - 2017 NotPetya Attacks
  - 2018 Olympic Destroyer South Korea
  - 2022 Linked to HermeticWiper


Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact

Wizard Spider

Sandworm

Common

3 Evaluation Scenarios:

- Day 1: Detection Wizard Spider TTPs
- Day 2: Detection Sandworm TTPS
- Day 3: Protection combined TTPS

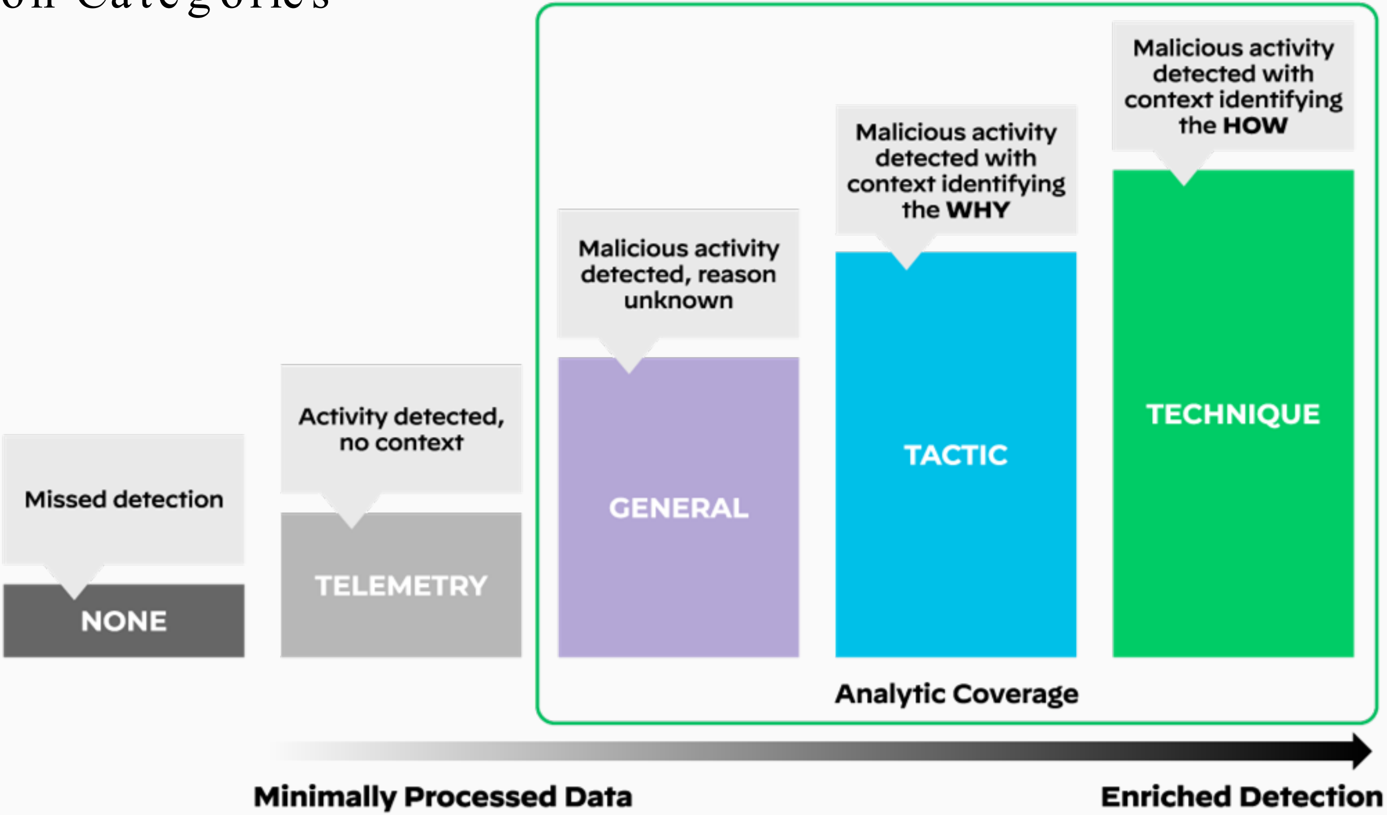
Detection: 19 Attack Steps and 109 substeps
Protection: 9 Attack Steps

Enterprise 4 Evaluations

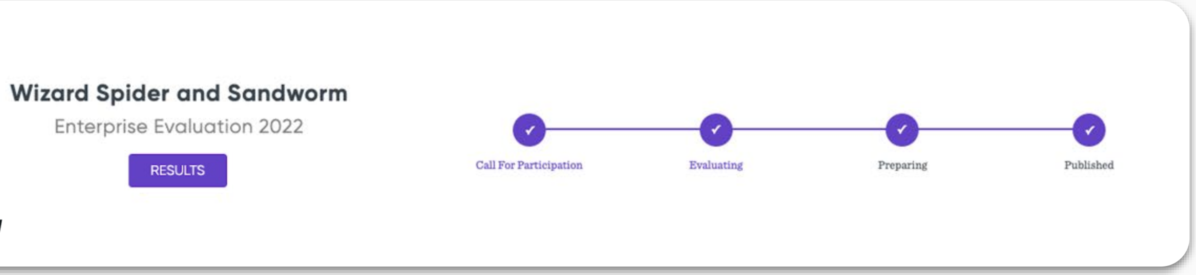
Cortex XDR Results

MITRE Engenuity

Detection Categories


Missed detection
NONE
Activity detected, no context
TELEMETRY
Malicious activity detected, reason unknown
GENERAL
Malicious activity detected with context identifying the **WHY**
TACTIC
Malicious activity detected with context identifying the **HOW**
TECHNIQUE
Analytic Coverage
Minimally Processed Data
Enriched Detection

MITRE Engenuity Enterprise 4 ATT&CK Evaluation Results: Cortex XDR



Wizard Spider and Sandworm

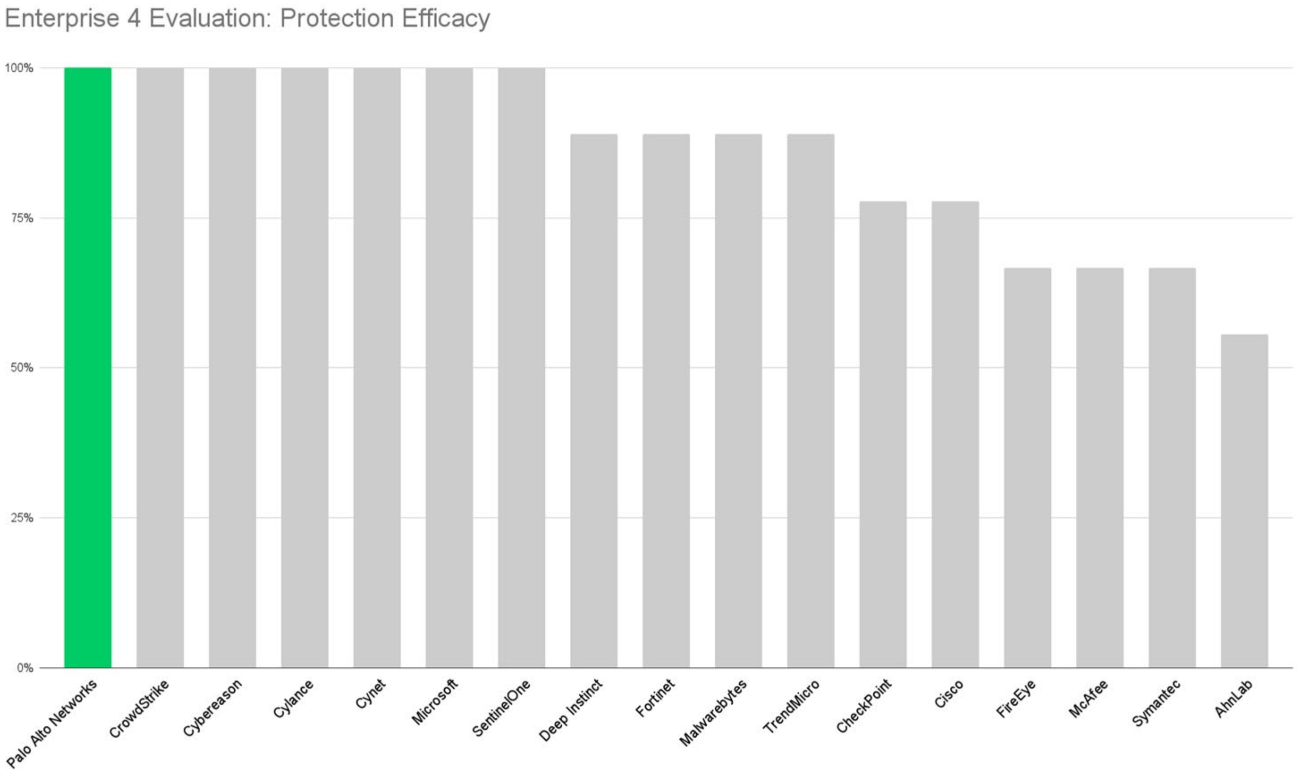
Enterprise Evaluation 2022

Cortex XDR Results:

- **100% Prevention** in the Protection evaluation (9 of 9)
- **100% Detection** of all attack steps (19 of 19)
- **98.2% Analytic Coverage** (107 of 109 attack substeps)
- **98.2% Technique-Level Detections** (107 of 109 attack substeps)
- **98.2% Visibility** (107 of 109 attack substeps)

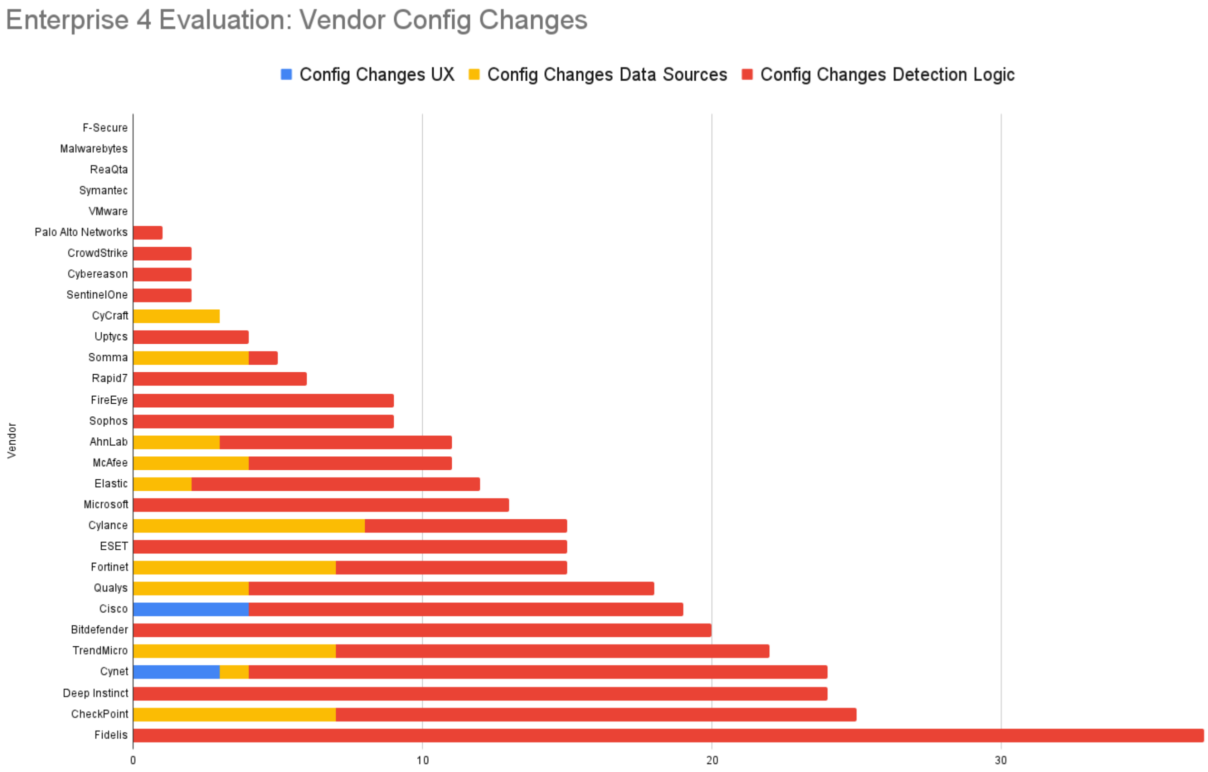
Protection Evaluation

Enterprise 4 Eval: Protection



Out of the Box Results (Config Changes Excluded)

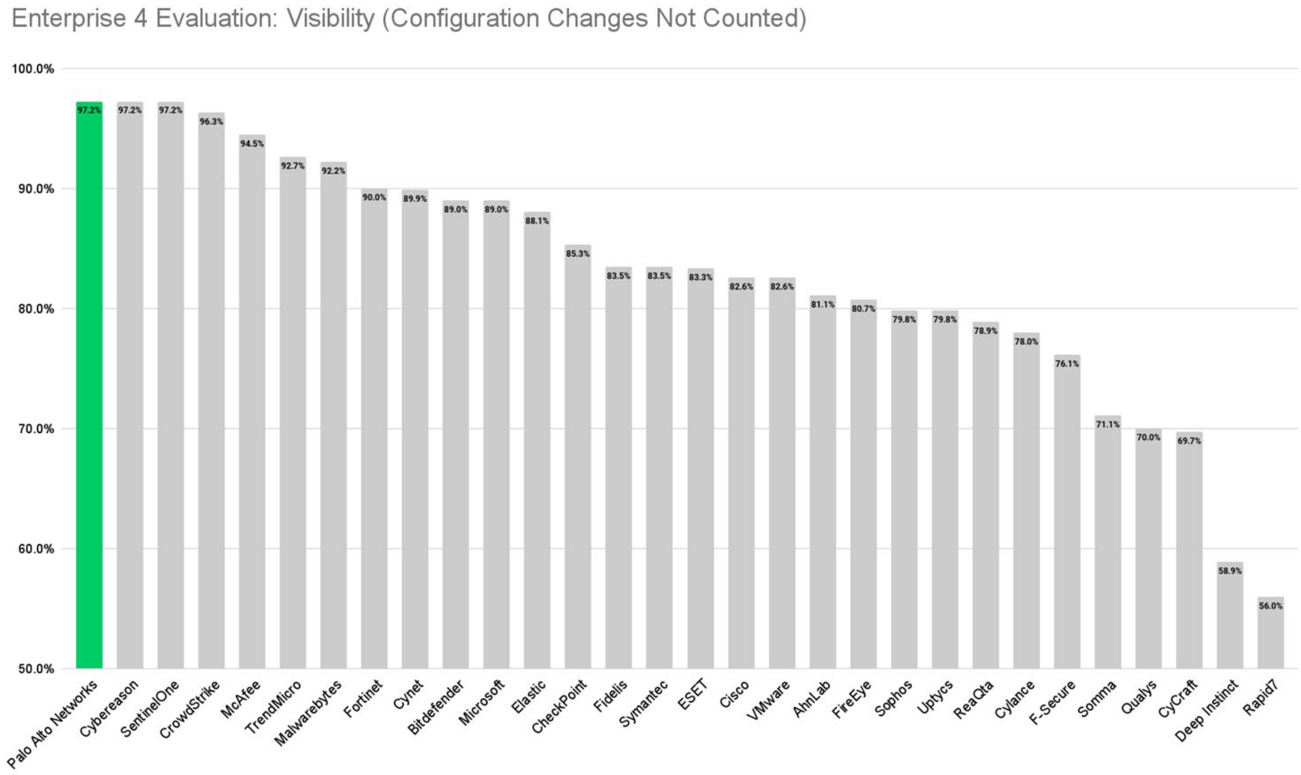
Configuration Changes



MITRE Engenuity identified detections that were based on configuration changes.

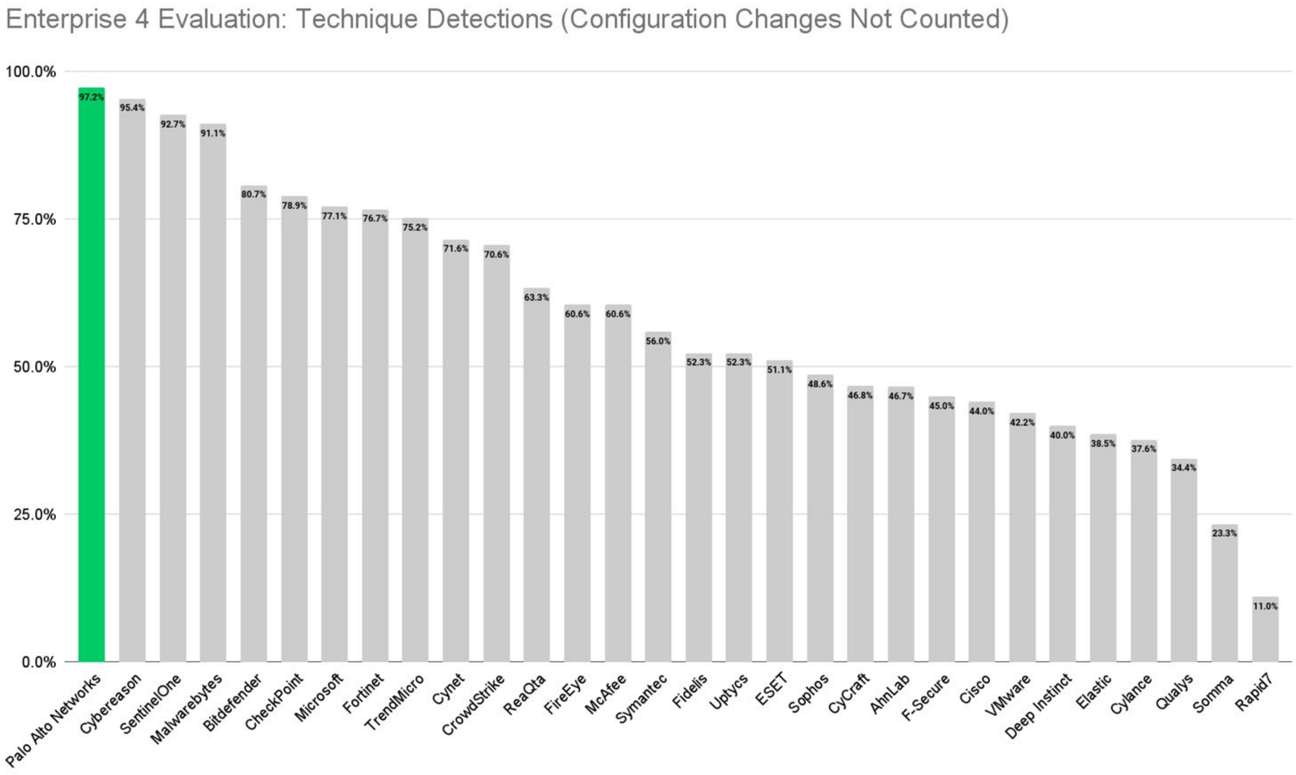
Be wary of solutions that required a high number of configuration changes to produce their results.

Enterprise 4 Eval: Visibility (Config Changes Excluded)



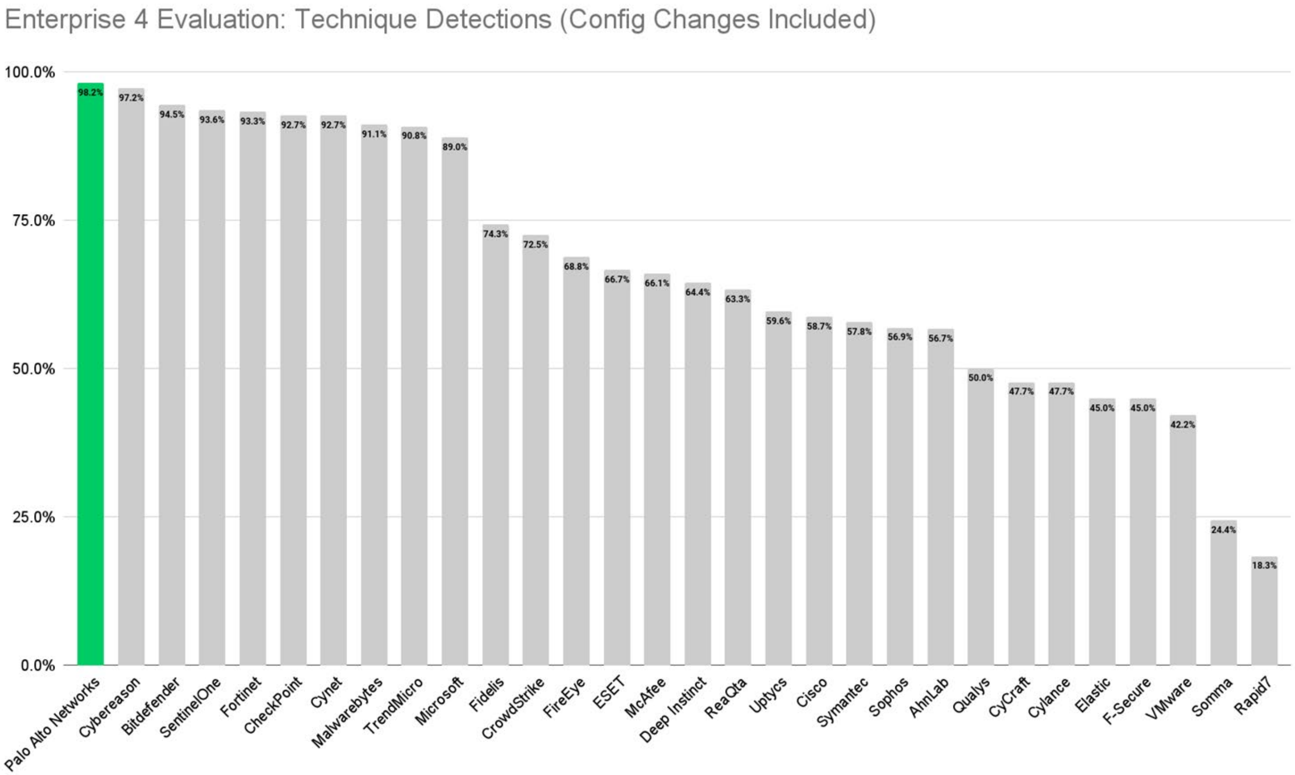
Enterprise 4 Evaluation: Visibility (Configuration Changes Not Counted)

Enterprise 4 Eval: Technique Detections (Config Changes Excluded)


Enterprise 4 Evaluation: Technique Detections (Configuration Changes Not Counted)

Configuration Changes Included

Enterprise 4 Eval: Technique Detections (With Config Changes)



Enterprise 4 Evaluation: Technique Detections (Config Changes Included)

Cortex XDR and Cortex XSOAR

Why SecOps Teams Need a New Approach

Too many alerts

11,047

alerts a day

Too many tools

45

point products

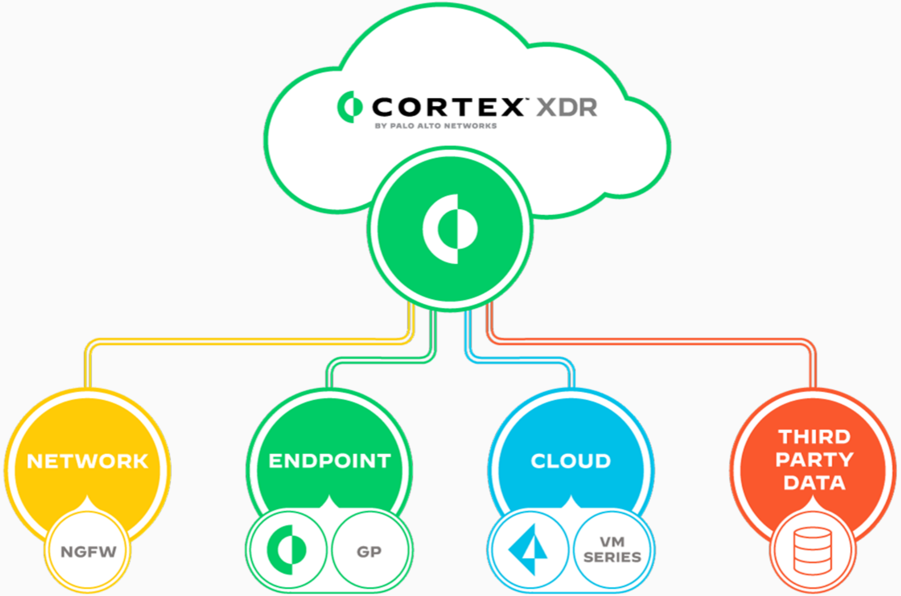
Too many missed attacks

$4.2M

average cost of a breach

31.2%

Cortex XDR Stops Ransomware & Advanced Threats

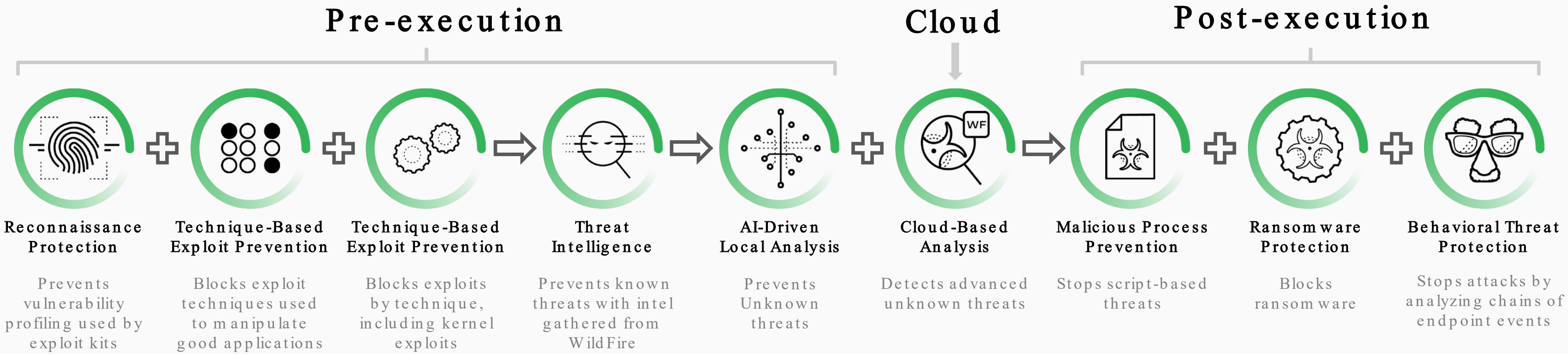


Find stealthy attacks with AI & cross-data analytics

Quickly investigate with root cause analysis

Contain any threat with coordinated response

Comprehensive Endpoint Protection



Pre-execution

Cloud

Post-execution

Reconnaissance Protection

Prevents vulnerability profiling used by exploit kits

Technique-Based Exploit Prevention

Blocks exploit techniques used to manipulate good applications

Technique-Based Exploit Prevention

Blocks exploits by technique, including kernel exploits

Threat Intelligence

Prevents known threats with intel gathered from WildFire

AI-Driven Local Analysis

Prevents Unknown threats

Cloud-Based Analysis

Detects advanced unknown threats

Malicious Process Prevention

Stops script-based threats

Ransomware Protection

Blocks ransomware

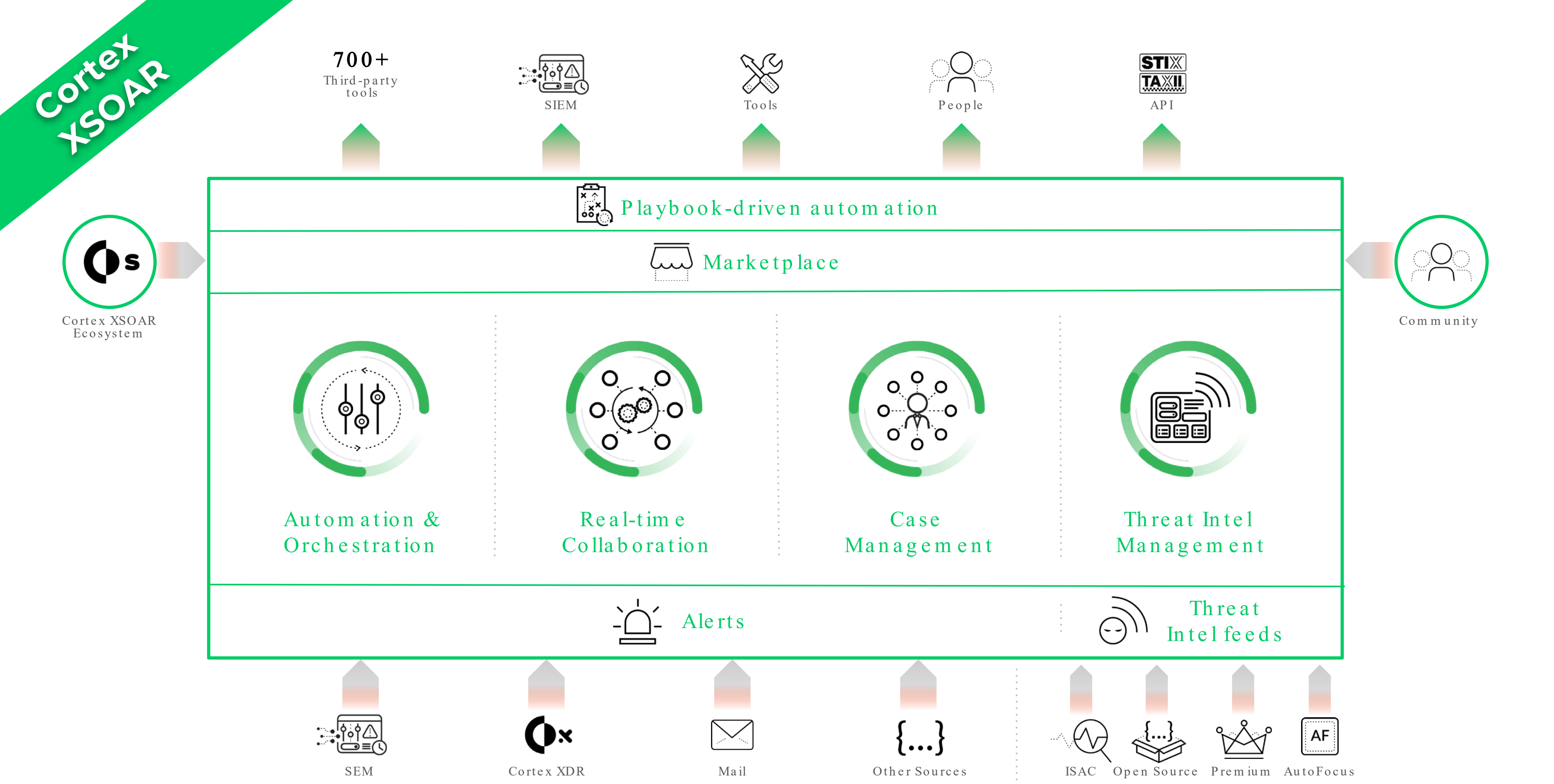
Behavioral Threat Protection

Stops attacks by analyzing chains of endpoint events

Device control, disk encryption and firewall reduce attack surface

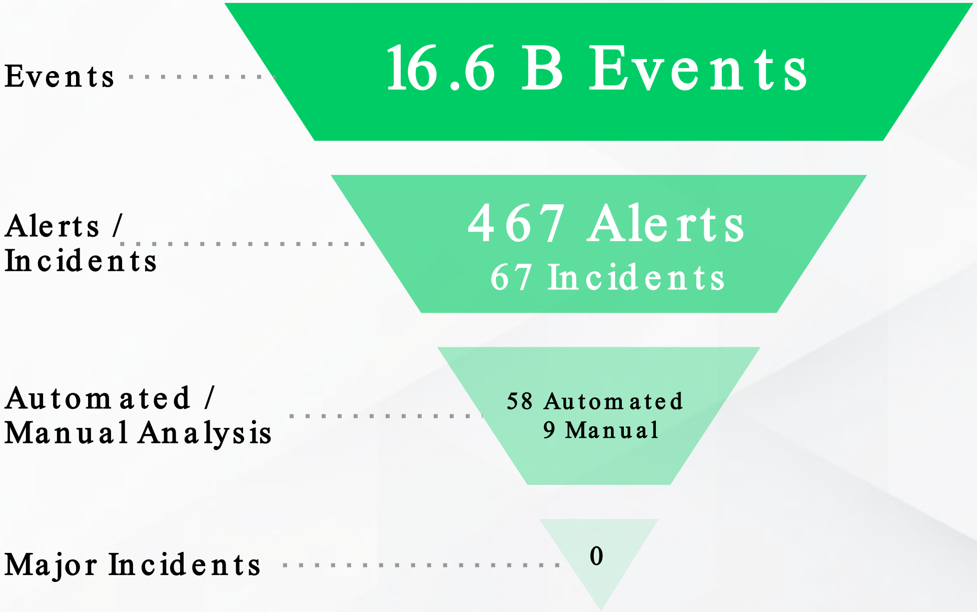
Optional AV scanning and on-prem broker for compliance

Behavioral Threat Protection to block evasive & fileless attacks


Cortex XSOAR
700+
Third-party tools
SIEM
Tools
People
STIX
TAXII
API
Playbook-driven automation
Marketplace
Cortex XSOAR Ecosystem
Community
Automation & Orchestration
Real-time Collaboration
Case Management
Threat Intel Management
Alerts
Threat Intel feeds
SEM
Cortex XDR
Mail
{...}
Other Sources
ISAC
{...}
Open Source
Premium
AF
AutoFocus

Palo Alto Networks SOC achieves a 1-minute response time

DAY IN THE LIFE OF THE PALO ALTO NETWORKS SOC



Events: 16.6 B Events

Alerts / Incidents: 467 Alerts, 67 Incidents

Automated / Manual Analysis: 58 Automated, 9 Manual

Major Incidents: 0

10 SECONDS

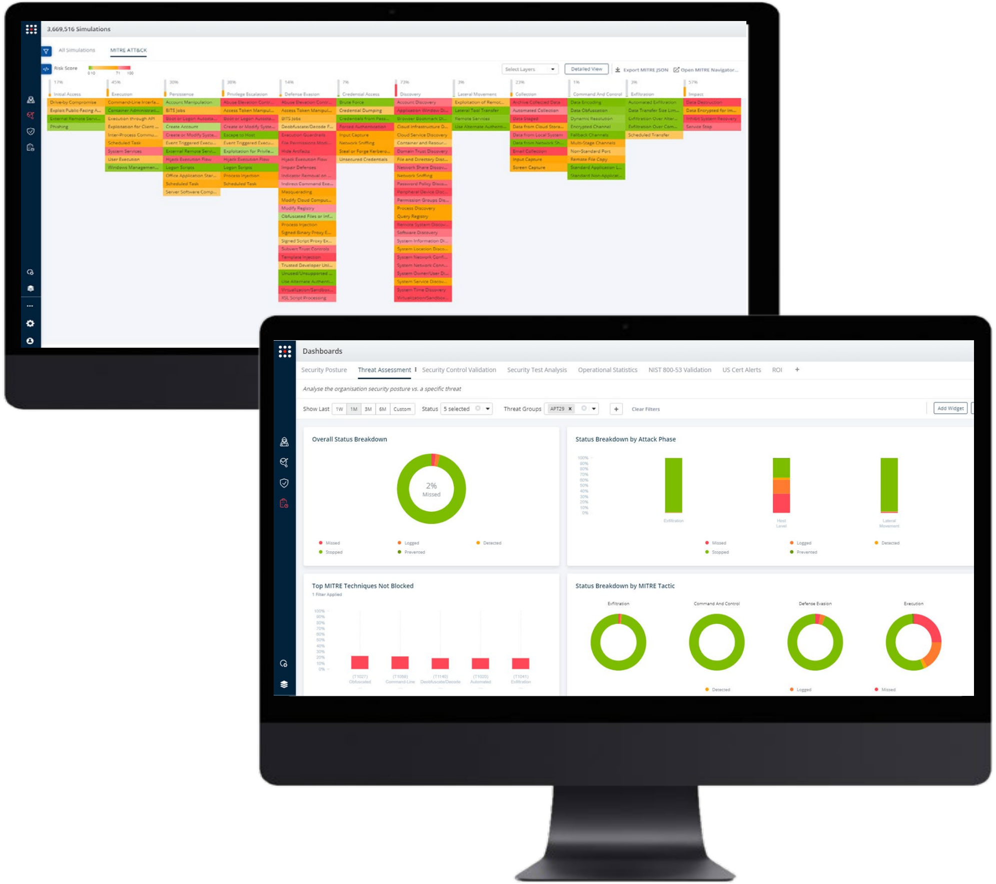
Mean Time to Detect

1 MINUTE

Mean Time to Respond
(High priority)

Palo Alto Networks Cortex and SafeBreach

Visualize Your Posture with MITRE ATT&CK Details



Analyse the organisation security posture vs. a specific threat

- MITRE ATT&CK Heat Map
- Risk Score
- Explorer View of Kill Chain
- Executive Dashboards

SafeBreach - Cortex XSOAR Integration

Closed-Loop Automated Breach Remediation

Discover security gaps
with continuous
breach simulation

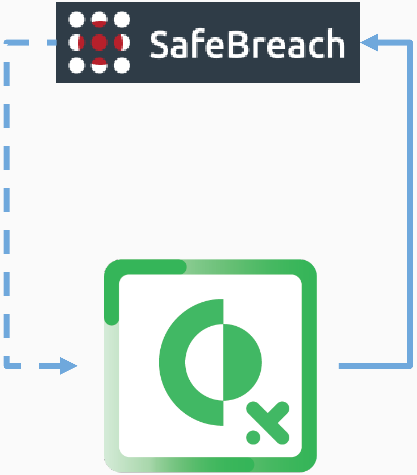
Remediate and validate
missed IOCs
automatically

Maximize the value
of your existing
security controls

SafeBreach + CORTEX XSOAR BY PALO ALTO NETWORKS

Cortex XDR and SafeBreach Integration

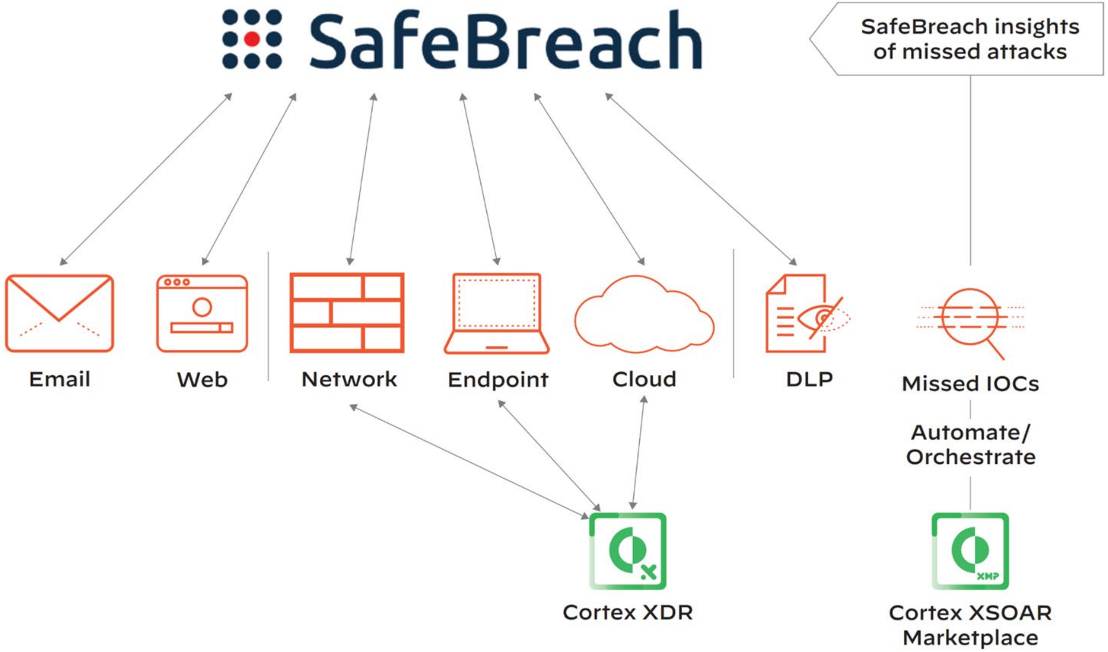
1. SafeBreach simulates attacks that trigger Cortex XDR rules



2. Security events collected and security action validated

- Provide unparalleled visibility into endpoint security performance
- Continuously execute attacks to baseline, monitor, and detect any deviation in coverage.
- Optimize endpoint configurations with SafeBreach Insight remediations.

Simplify Configuration Updates with Cortex XSOAR & Cortex XDR



- Automate test attacks against Cortex XDR endpoints with a Cortex XSOAR content pack:
  - Identify which IOCs were not blocked
  - Automatically remediate unblocked IOCs
  - Rerun attack scenarios to ensure all security gaps are addressed.
- Streamline configuration updates with XSOAR playbooks.

Questions?

Thank You

SYMPHONY
2022

May 18, 2022 | 9am PDT

presented by:

paloalto NETWORKS | CORTEX BY PALO ALTO NETWORKS