Cortex Forensics

In today's evolving threat landscape, security teams need deep forensic visibility to quickly investigate incidents, uncover hidden threats, and prevent future attacks. Security professionals should be able to proactively hunt for threats using historical endpoint artifacts and respond quickly to incidents with complete visibility into adversary actions. From postbreach analysis to in-depth forensic investigations, Cortex® Forensics unifies the essential data, streamlined workflows, and real-time detection and response capabilities from Cortex needed to accelerate investigations, contain threats, and enhance the overall security posture.

Cortex Forensics Benefits:

- **Faster response with less effort:** Accelerate incident response by quickly accessing and processing robust artifact packages without needing complex queries.
- **Level-up your Cortex investigations:** The Forensics module provides a deeper, historical, and complete layer of investigation on top of the Cortex platform.
- **One place for all your data:** Collect and analyze forensic data from online, offline, and air-gapped endpoints and different OSs with complete artifact packages.
- **Staying one step ahead with proactive hunting:** Uncover hidden threats using historical forensic data for early detection and response.

The Cortex Investigation Experience

Built as part of the Cortex platform, Cortex Forensics provides an end-to-end solution, helping you with every step of incident investigation including data collection, analysis, and threat hunting. Incident responders can review evidence, hunt down threats, and perform compromise assessments from a single console. And, with instant access to a wealth of forensic artifacts, your team can determine the source and scope of an attack and what, if any, data was accessed.

All the Data You Need at Your Fingertips

Analyze key artifacts—such as event logs, registry keys, and browser history—to quickly pinpoint attacker activity. Fully investigate details for each entry with the host timeline view and uncover remnants of malware, even for deleted files, with program execution artifacts. With Cortex Forensics, you have a complete picture of an endpoint, including full file listings of all connected drives.

A Converged Platform for Analysis and Response

Make swivel-chair syndrome a thing of the past by unifying detection, response, and forensic analysis in a single console. You can view forensic evidence, endpoint events, network data collected from your firewalls, authentication events, and more. The forensic data can be viewed across the Cortex platform, including the causality chain. Unlike siloed forensic tools, your analysts can monitor activity and verify threats from one console, including activity from unmanaged endpoints and IoT devices.

Once your team has verified a threat, they can contain threats quickly with a coordinated response. Stop the spread of malware, restrict network activity to and from devices, or sweep across all endpoints in real time with Search and Destroy. The powerful Live Terminal feature lets analysts shut down attacks without disrupting end users by directly accessing endpoints and running Python, PowerShell, system commands and scripts, and managing endpoint files and processes.

Post-Breach Triage and Incident Response

Rapidly understand incidents so teams can respond effectively with comprehensive data collection from endpoints after an incident occurs, providing unparalleled visibility into what happened and when. Like dusting for fingerprints at a crime scene, investigators can install the Cortex agent as part of their forensic investigation to retroactively collect rich endpoint details, including historical information dating back weeks or months before the incident. Using the forensic triage functional-

ity, investigators can focus on collecting the most relevant forensic artifacts, such as full file listings, complete event logs, full registry hives, supported forensic artifacts, and user-defined file collections. By focusing on these artifacts, you get faster results without the delays of full-disk imaging.

Forensic Hunting for Expanded Insights

Threat hunting teams can expand their investigation by searching historical artifacts for evidence of malicious or suspicious behavior with the dedicated forensic hunt flow shown in figure 1. The forensic hunt flow provides the flexibility to define and filter artifact searches and periodic queries based on custom criteria. By analyzing historical evidence, investigators can identify potential risks or activities. This enables each hunter to create tailor-made collections and hunt queries based on their knowledge of the organization's threat landscape and infrastructure.

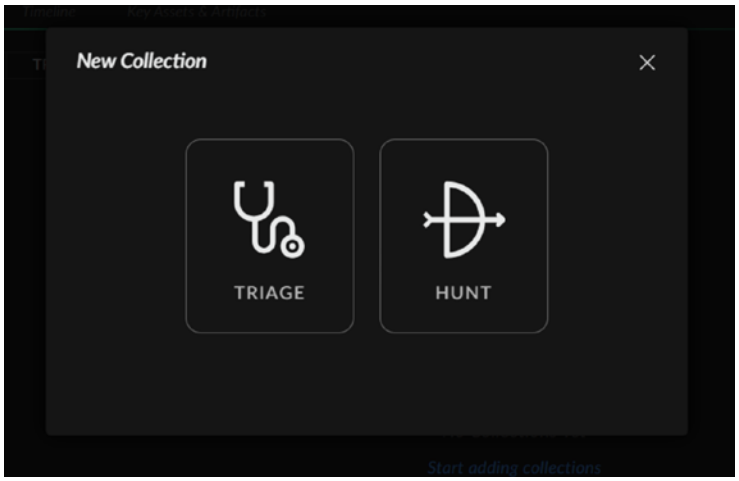

Figure 1. Proactive and reactive investigation flows for hunters

Analysis of Offline or Air-Gapped Endpoints

When you suspect an endpoint has been compromised, your first step is to isolate the endpoint from the network. However, you still need to verify suspicious activity, examine which files might have been accessed, and eliminate all traces of the threat. With Cortex Forensics, you can investigate offline or air-gapped endpoints by downloading a complete forensic snapshot of an endpoint and then uploading it to Cortex for analysis.

Memory Collections

Memory analysis can provide insights that disk-based forensics cannot. Want to analyze an in-memory malware module or extract the command history from a running console? Collecting memory from an impacted host can give you greater visibility into attacker activity, providing the investigator access to volatile artifacts that might never be written to disk.

Cortex Forensics supports the collection of memory images from Windows systems—from online hosts via the Action Center or offline hosts via the offline triage collector. Memory images are captured in a raw format compatible with all major memory analysis tools.

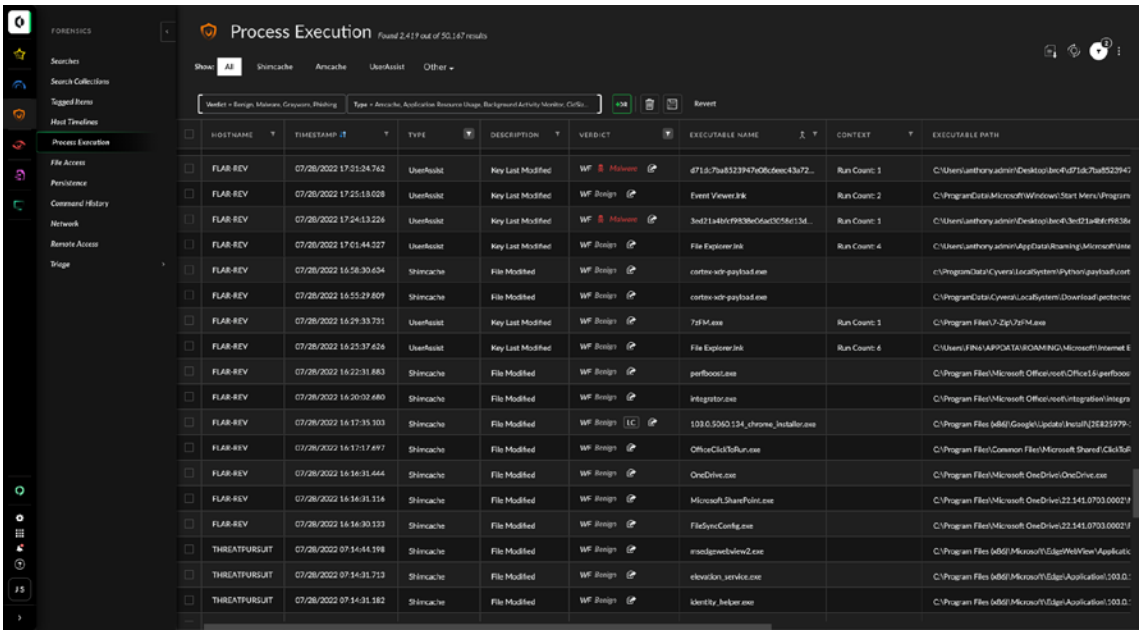

Figure 2. Easy-to-consume presentation of the artifacts

Proven Detection and Response

Cortex Forensics enhances your security operations by seamlessly integrating forensic data with real-time detection and response from Cortex, providing faster threat containment and deeper investigative insights.

The forensics module played a critical role in detecting the Lazarus attack, resulting in the highest combined protection and detection rates in the MITRE ATT&CK Round 6 Evaluations. With the unsurpassed security score from Cortex in the AV-Comparatives Endpoint Prevention and Response Test, and leadership positions in the Gartner® EPP Magic Quadrant™ and the Forrester Wave™ for XDR Providers, be assured you're receiving the best possible endpoint security from Cortex.

Palo Alto Networks Unit 42®—a world-recognized incident response, threat intelligence, and security consulting organization—enables you to respond swiftly and contain threats completely so you can get back to business quickly. Unit 42 consultants use the forensics module for real-life investigations, court cases, and regulatory reports. Take advantage of the same forensics solution used by our Unit 42 team of experts.

Learn More

Do you want to see Cortex Forensics in action? Schedule a demo today, or visit the webpage to learn more.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

cortex_ds_cortex-forensics_053025