Resecurity

Resecurity HUNTER

Managed Threat Analysis

The Challenge

Threat actors continually change the way they avoid detection, and many of them use artificial intelligence (AI) and machine learning (ML) to intelligently deploy attacks. Organizations are under constant pressure to find new threats and create a system that defends against a wide range of adversarial techniques that mutate frequently.

Manual methods of finding threats are inefficient and leave detection vulnerabile to possible human errors. It requires expertise often not found within the organization. Not only is human expertise hard to find, but configuring software solutions also requires an expert familiar with the right data collection and analysis settings.

Proactive Threat Hunting

Armed with Resecurity Hunter, organizations have the power of autonomous threat analysis and deep analysis of traffic patterns, user behaviors, and potential vulnerabilities. Our threat analysis software proactively monitors and detects user, application, system and network anomalies.

Resecurity Hunter works with large datasets of collected information to pinpoint advanced threats and respond to today's complex cyber-attacks that commonly evades detection. Organizations get full analysis, reporting, details and remediation recommendations for effective cybersecurity against today's advanced attacks.

MANAGED THREAT HUNTING

Combine raw organizational data with Resecurity's AI analytical software to process large silos of network traffic information and uncover complex threats.

EXTRACT SIGNALS FOR REVIEW

Connect Resecurity Hunter with current data analysis and collection applications to extract threat signals for further review.

Hunter reports tell a story that can be used to further understand risks and the organization's attack surface.

DISCOVER HIDDEN THREATS

Detect hidden threats evading current monitoring tools across firewalls, cloud storage, servers, desktops, user devices, and other network infrastructure.

GET IN-DEPTH ANALYSIS

Use our AI in-depth analysis to discover indicators of compromise (IoC) to reveal threats and isolate them.

Analysis reports provide better insight into potential threat activity and network actions.

ACTIONABLE GUIDANCE

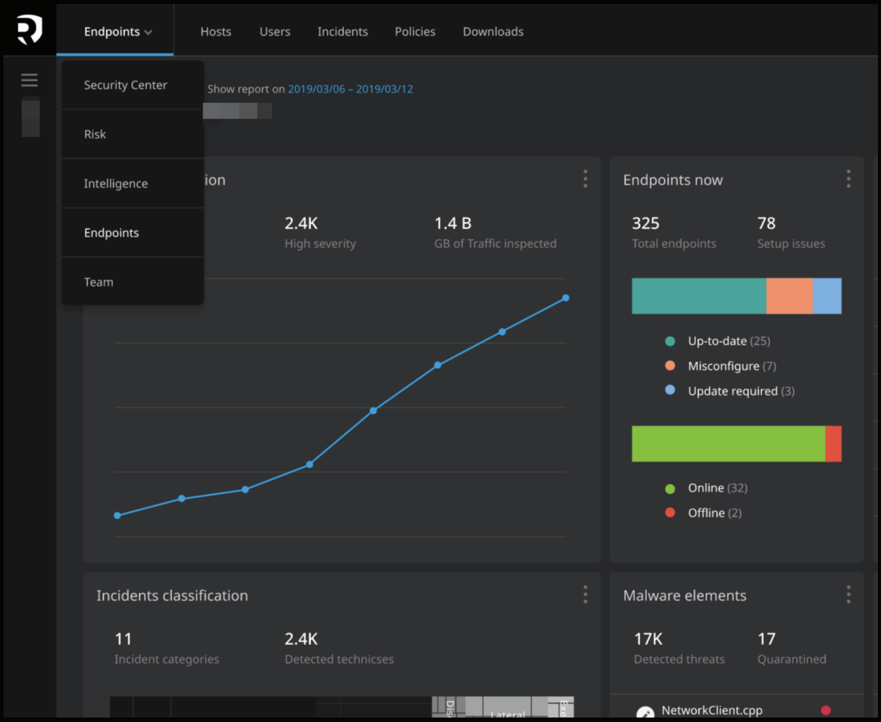
Deploy strategies across your environment based on the actionable guidance provided by Hunter analysis and reduce remediation and incident response times.

STAY COMPLIANT

Avoid compliance issues and hefty fines by identifying misconfigurations and insider threats.

Stay compliant with detailed reports where improvements could be made.

Resecurity



Show report on 2019/03/06 – 2019/03/12

2.4K High severity

1.4 B GB of Traffic inspected

Endpoints now

325 Total endpoints

78 Setup issues

- ● Up-to-date (25)
- ● Misconfigure (7)
- ● Update required (3)

- ● Online (32)
- ● Offline (2)

Incidents classification

11 Incident categories

2.4K Detected technicses

Malware elements

17K Detected threats

17 Quarantined

Alerts For

- Suspicious outbound TCP traffic
- Executable files written to network disks
- DLL files written to network disks
- Suspicious inbound TCP traffic
- Launched executables from sensitive locations
- System configuration changes
- Misconfigurations
- System and network service changes
- Email attachment execution and storage
- Users browsing suspicious
- URLs and domains
- Data exfiltrated to FTP servers
- Outbound file transfers
- Microsoft Office suspicious active such as malicious macros
- Indicators of Compromise (IoC)
- Windows Registry changes
- Authentication requests success and failures

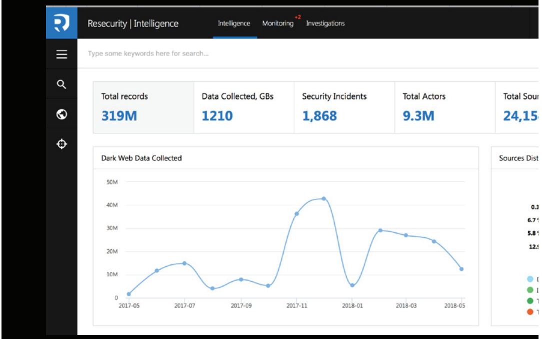
Benefits

- Scaled threat hunting for enterprise organizations with large attack surfaces.
- Leverage logs and audit trails as sources for data-driven identification of hidden threats.
- Find threats that bypass authentication and authorization controls.
- Use AI to autonomously detect ongoing attacks and isolate them before they become a critical data breach.
- Reduce false positives using Hunter's data-driven analysis and detection.
- Eliminate administrator overhead and workloads and improve incident response times.

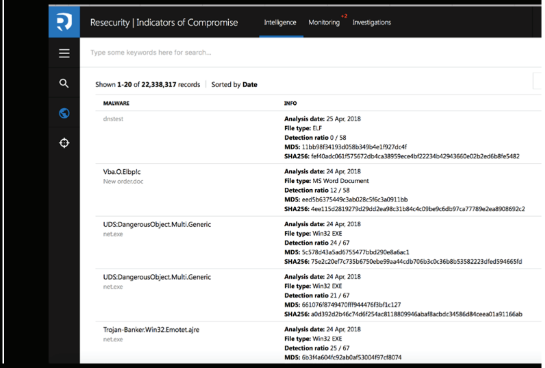
Key Features

- Millions of data points from collected network traffic used to detect threat signals across any platform.
- Autonomous threat hunting means reduced human intervention and better analytical reports.
- Translate Hunter findings into actionable remediation strategies.
- Hunter updates and "learns" from the latest data points and traffic patterns specific to your environment.
- Seamless integration with current enterprise infrastructure including cloud or on-premise.
- Integration into current SIEM environments.

Screenshots



Total records	Data Collected, GBs	Security Incidents	Total Actors	Total Sou
319M	1210	1,868	9.3M	24,15


Resecurity | Indicators of Compromise
Intelligence
Monitoring
+2
Investigations
Type some keywords here for search...

Shown **1-20** of **22,338,317** records | Sorted by **Date**

MALWARE	INFO
dnstest	**Analysis date:** 25 Apr, 2018 **File type:** ELF **Detection ratio** 0 / 58 **MD5:** 11bb98f34193d058b349b4e1f927dc4f **SHA256:** fef40adc061f575672db4ca38959ece4bf22234b42943660e02b2ed6b8fe5482
Vba.O.Elbp!c New order.doc	**Analysis date:** 24 Apr, 2018 **File type:** MS Word Document **Detection ratio** 12 / 58 **MD5:** eed5b6375449c3ab028c5f6c3a0911bb **SHA256:** 4ee115d2819279d29dd2ea98c31b84c4c09be9c6db97ca77789e2ea8908692c2
UDS:DangerousObject.Multi.Generic net.exe	**Analysis date:** 24 Apr, 2018 **File type:** Win32 EXE **Detection ratio** 24 / 67 **MD5:** 5c578d43a5ad6755477bbd290e8a6ac1 **SHA256:** 75e2c20ef7c735b6750ebe99aa44cdb706b3c0c36b8b53582223dfed594665fd
UDS:DangerousObject.Multi.Generic net.exe	**Analysis date:** 24 Apr, 2018 **File type:** Win32 EXE **Detection ratio** 21 / 67 **MD5:** 661076f8749470fff944476f3bf1c127 **SHA256:** a0d392d2b46c74d6f254ac8118809946abaf8acbdc34586d84ceea01a91166ab
Trojan-Banker.Win32.Emotet.ajre net.exe	**Analysis date:** 24 Apr, 2018 **File type:** Win32 EXE **Detection ratio** 25 / 67 **MD5:** 6b3f4a604fc92ab0af53004f97cf8074

Resecurity www.resecurity.com info@resecurity.com (800) 781-5698 445 S. Figueroa Street, 31st Floor, Los Angeles CA 90071, USA.