INTEZER ANALYZE

for

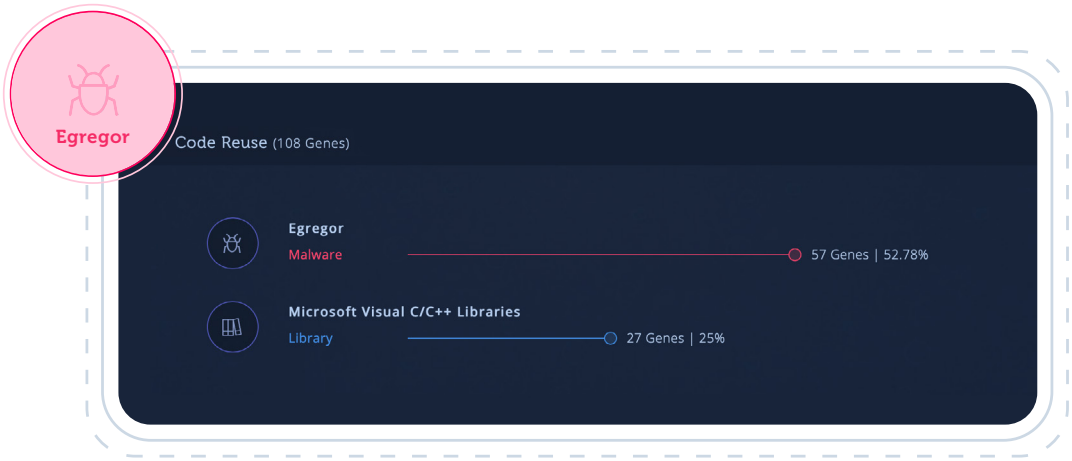
Managed Security Service Provider (MSSP)

One Platform for Malware Analysis and DFIR

- Classify malware in seconds
- Accelerate memory forensics
- Reduce false positives
- Proactive threat hunting

The Evolution of Threat Detection

Intezer detects threats by recognizing even the slightest amount of code reuse.



66

CTO, Global Managed Security Service Provider

Truly a game changer in a time when old guard capabilities of incident response and hunting are disappearing pushing towards a heavier reliance on technology.

99

Managed Detection & Response / SOC-as-a-Service

Whether you are monitoring the organization or investigating an incident after the fact, our investigation capabilities have an immediate impact.

Triage	Malware Analysis	Remediation	Threat Intelligence
Reduce false positives	Classify malware	Prioritize threats	Extract IOCs
Identify infected machines	Find related samples based on code reuse	Contain the attack	MITRE ATT&CK TTPs
Quickly assess damage to the organization	Automatic unpacking	Tailor response	Advanced YARA rules
	Analyze files, memory images and live machines	Prevent similar attacks in the future	Track malware families

Code Genome Database

66

Indicators can be easily extracted whether using submissions we provide or by looking at the extensive Genome Database Intezer has built, thus managing prevention measures with the incident response actions.

99

10 Billion+

Genes mapped in our database

10K+

Mapped threat actors and malware families

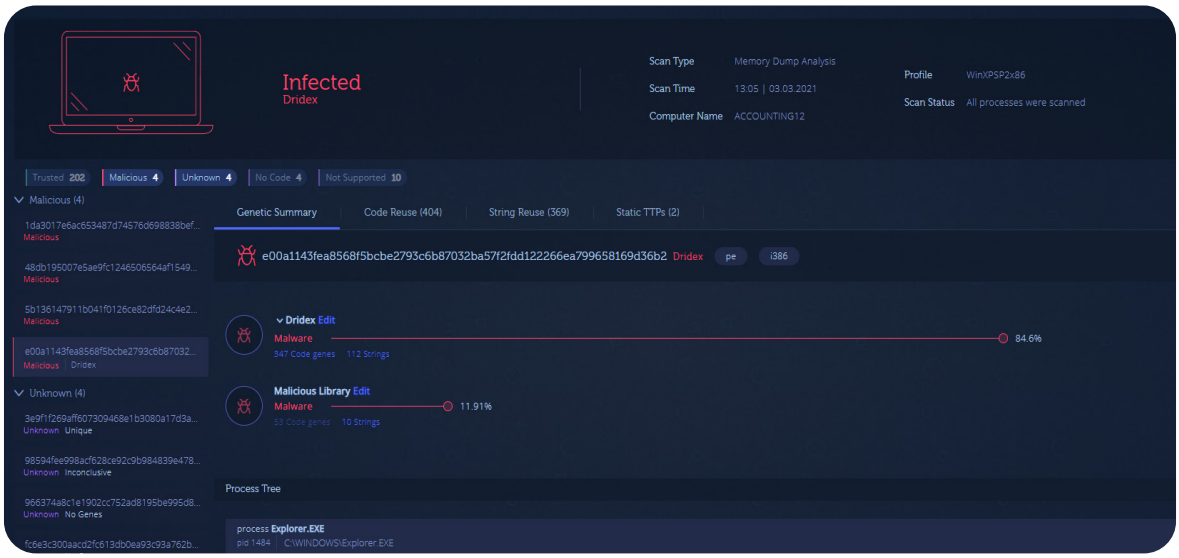
100K+

Mapped trusted applications and libraries

Accelerate Digital Forensics

Analyze live machines or entire memory dumps. Quick and accurate classification for every piece of code found in-memory.

Volatility plugin ***Memory dumps*** **Endpoint Scanner** ***Live machines***

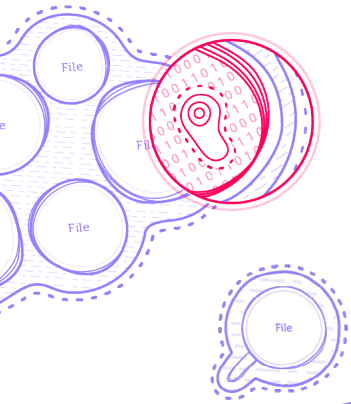


Proactive Threat Hunting

Predictable, recurring revenue stream for your business

SolarWinds and other attacks hid in networks for months without being detected. Actively scan the memory of your endpoints to identify advanced threats.

- Conduct immediate and periodical scans of your customers' endpoints to detect malicious code in-memory
- Detect malicious code injections, packed and multi-stage malware
- Verify all endpoints in the organization are running 100% trusted code



Contact Us