REnigma: A Tool to Analyze Malware

April 23, 2018

Julian Grizzard, Co-founder
James (Jim) Stevens, Co-founder

Deterministic Security, LLC

Spin-off of The Johns Hopkins University Applied Physics Laboratory

Need: Hard to Keep Networks Secure!

Attempt to stop attacks before they reach the end points	
Attempt to stop attacks that bypass network defenses	

Need: Hard to Keep Networks Secure!

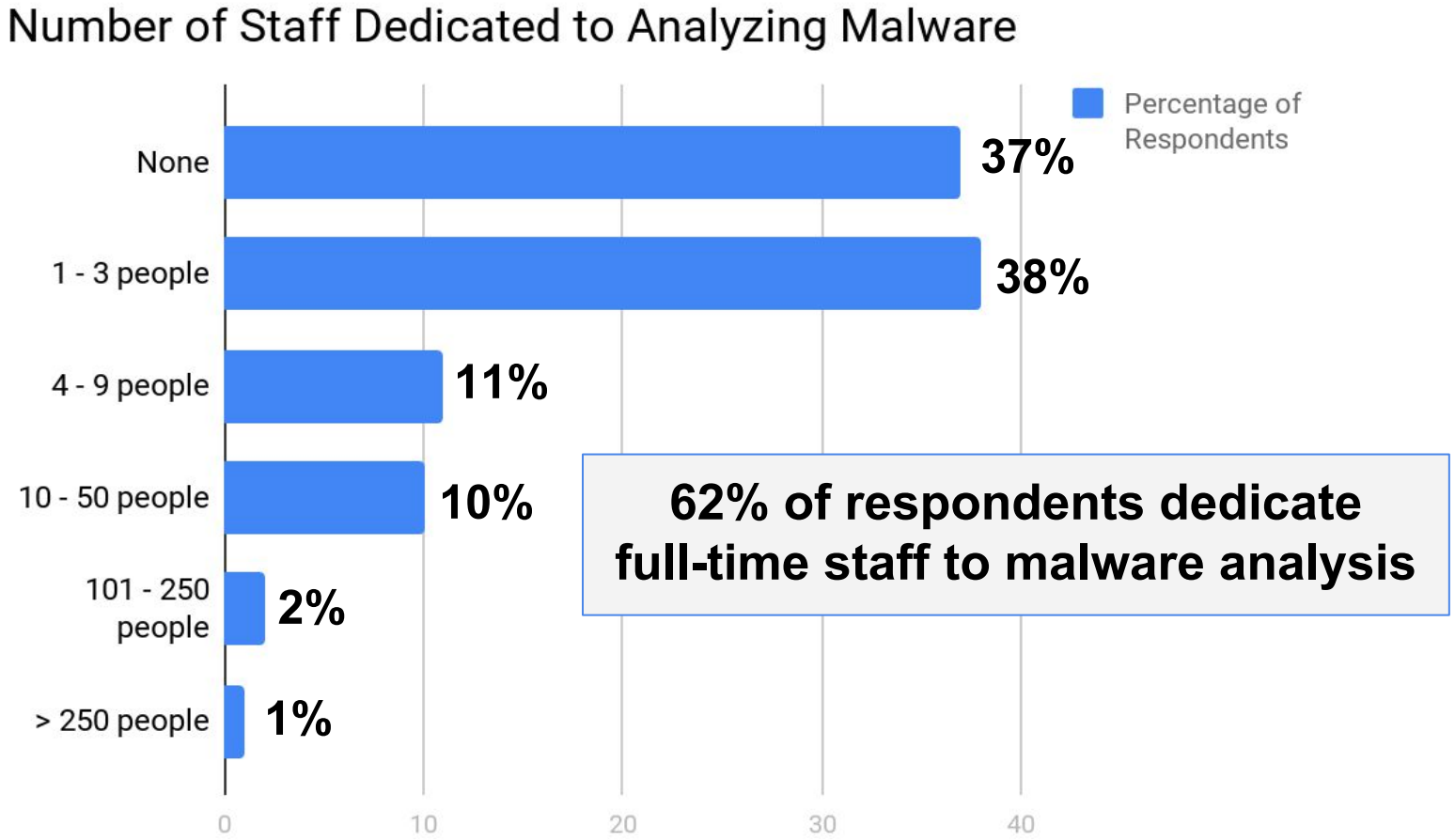
Attempt to stop attacks before they reach the end points	Network Defense
Attempt to stop attacks that bypass network defenses	End-Point Defense

- “PyeongChang 2018 Winter Olympics Opening Ceremony Disrupted by Malware Attacks”
- “Equifax Hack Exposes Personal Info of 143 Million US Consumers”

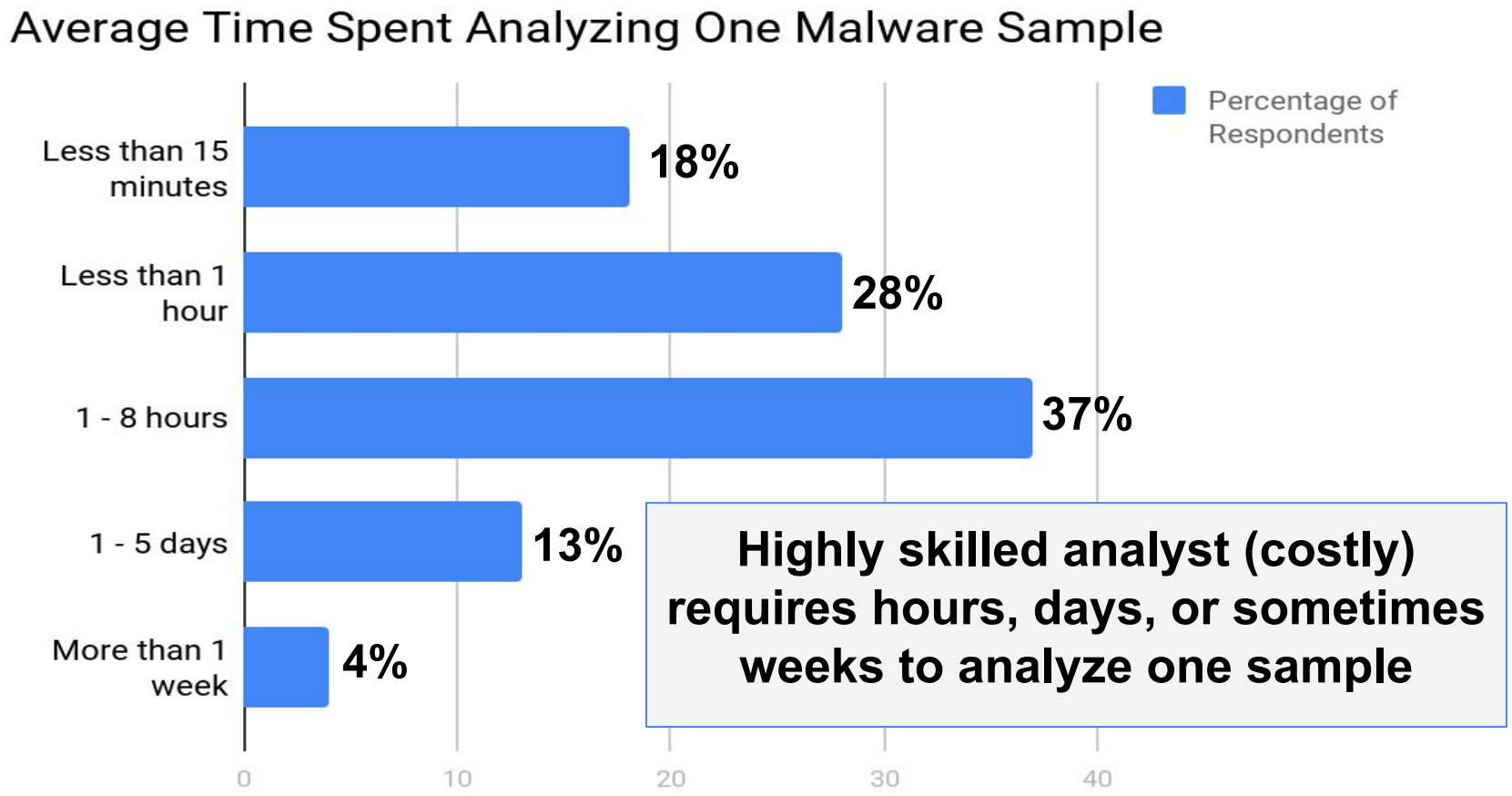
Threat and Incident Response

Incident Response Teams ● Recover from attacks that bypass all automated defenses	
Threat Teams ● Discover new threats and update defenses to block them	

REnigma focuses on threats that can make it through all automated defenses

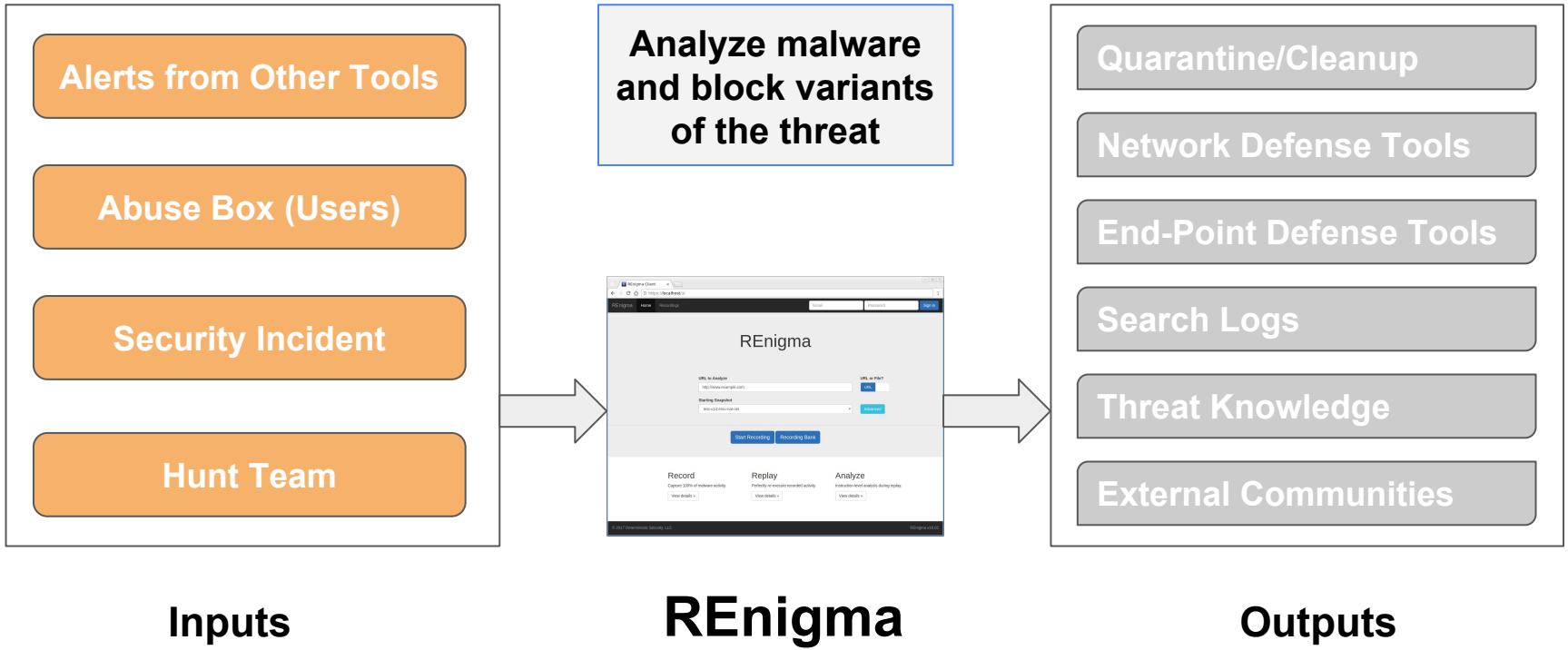


DHS-sponsored survey that includes Fortune 100, Fortune 500, S&P 500, Global 1000, and Global 2000 organizations (rounded)

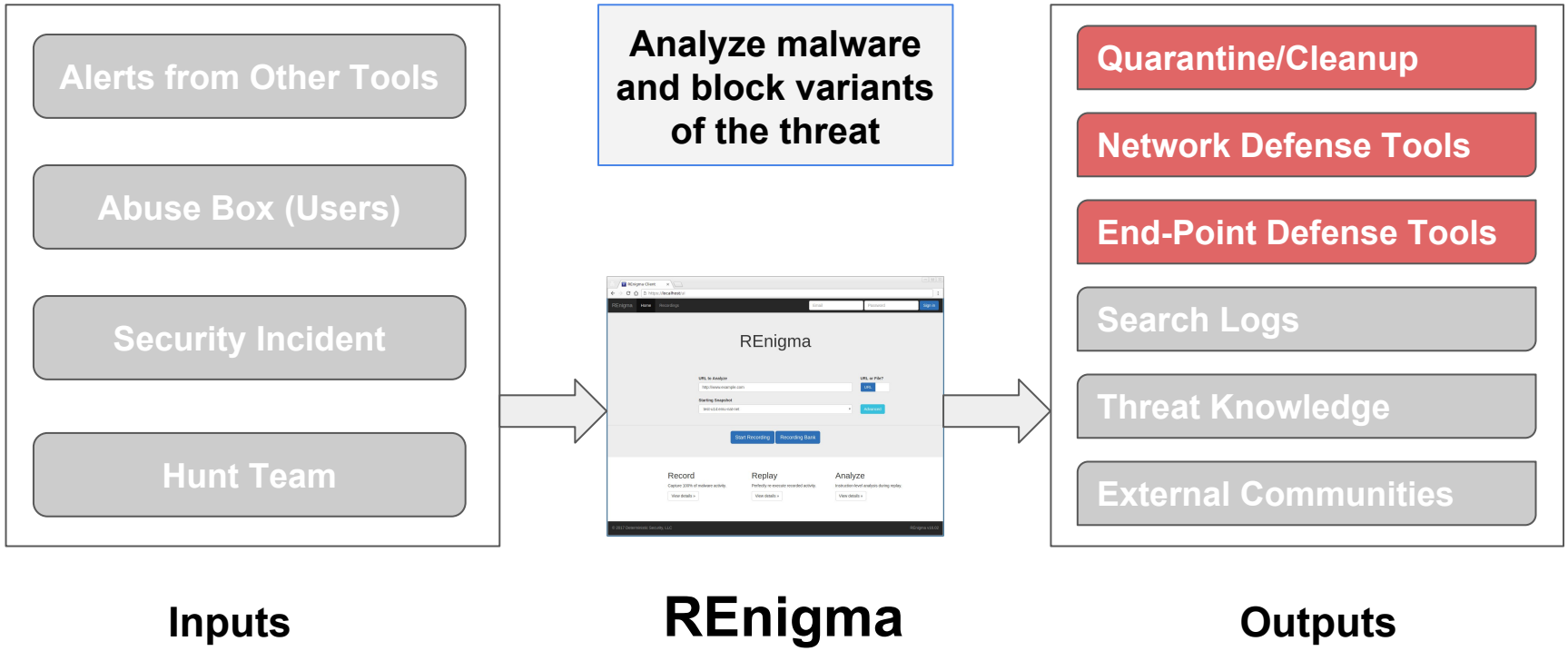


DHS-sponsored survey that includes Fortune 100, Fortune 500, S&P 500, Global 1000, and Global 2000 organizations (rounded)

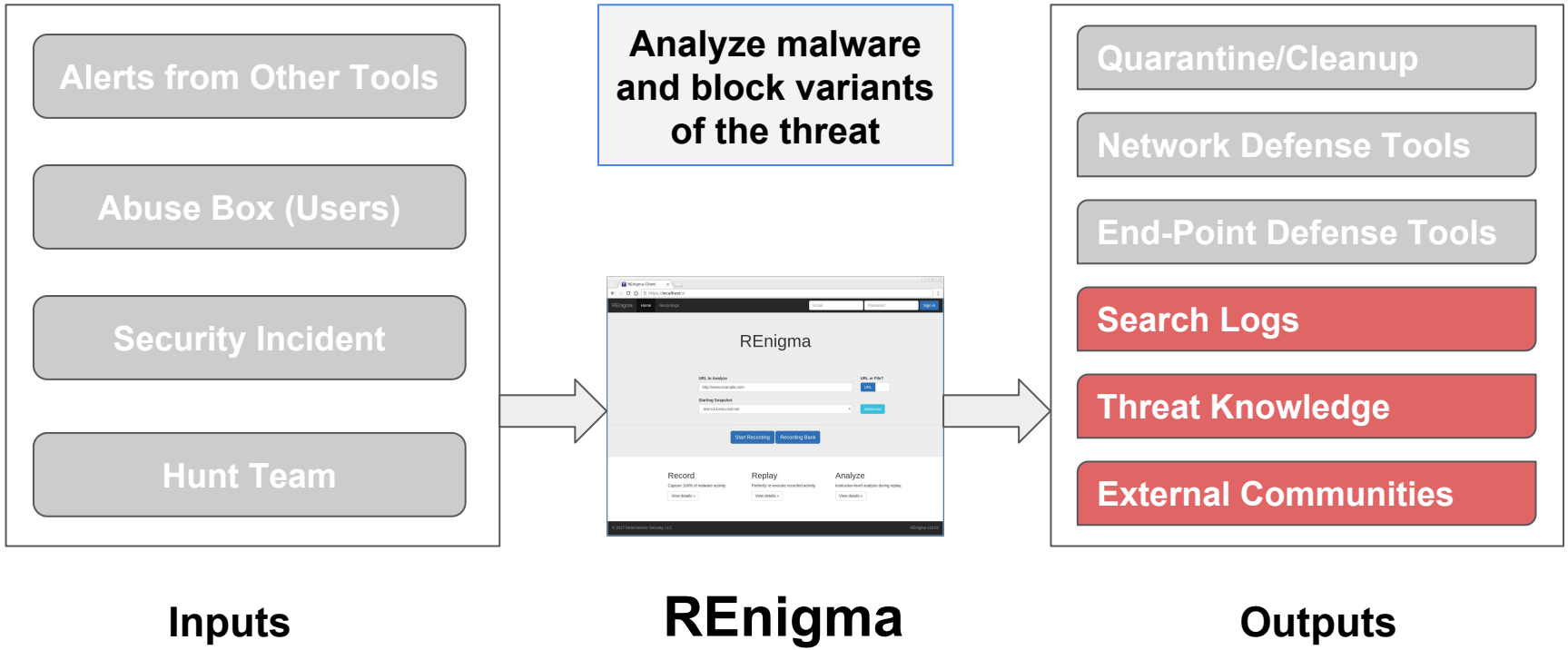
Approach - Overview



Approach - Overview



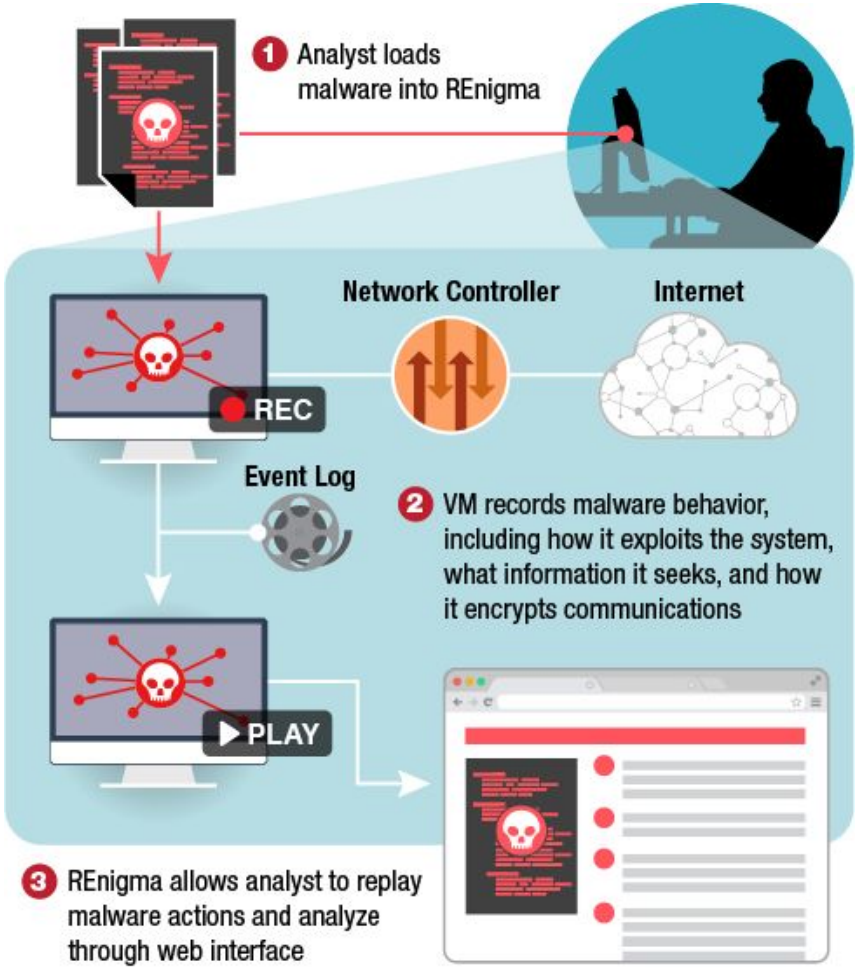
Approach - Overview



Approach - Analysis Detail

1. User uploads suspicious files or URLs to REnigma
2. REnigma records execution of sample in virtual machine (VM)
   - Interact with VM while recording
3. Analyst performs automated and/or semi-automated analysis of replay
   - Instruction-level analysis
   - “Rewind” to previous points

Output:
- **Deep understanding of threat**
- **Indicators of Compromise (IOCs)**

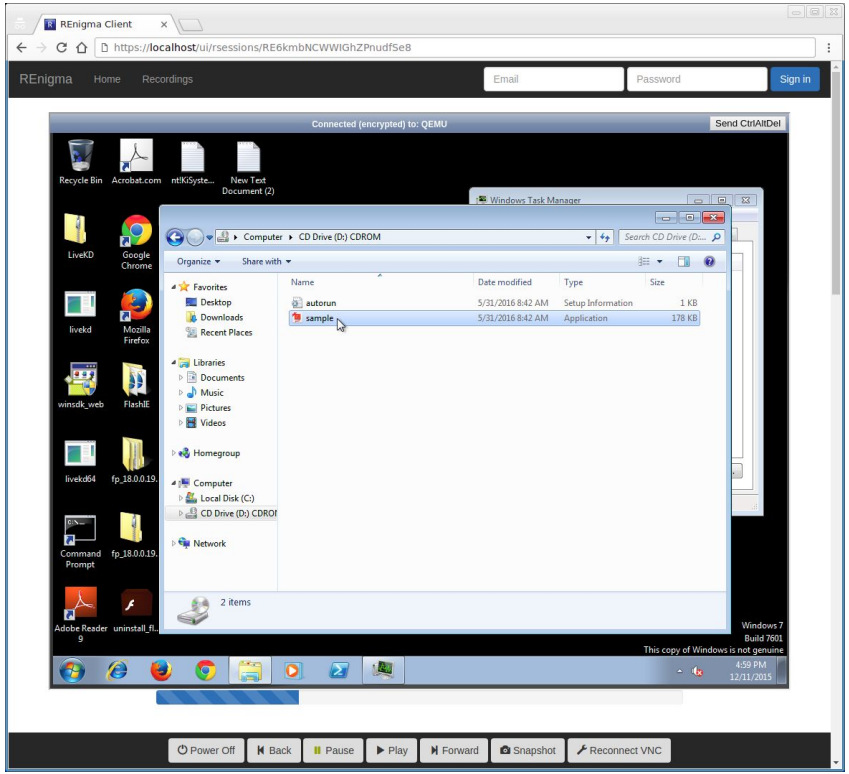


Approach - Analysis Detail

1. User uploads suspicious files or URLs to REnigma
2. REnigma records execution of sample in virtual machine (VM)
   - Interact with VM while recording
3. Analyst performs automated and/or semi-automated analysis of replay
   - Instruction-level analysis
   - “Rewind” to previous points

Output:

- **Deep understanding of threat**
- **Indicators of Compromise (IOCs)**



Benefits

- Record and replay functionality solves critical challenges in analysis
- Example: Easily “rewind” to point before cleanup

Quickly Understand New Threats

- Analyst often has only “one shot” to capture sample (e.g., website gone)
- Recording can capture sample before it is gone

Solve the “One Shot” Problem

- Export data in standard formats for analysis with existing tools
- Example tools: IDA Pro, Wireshark, Volatility

Leverage Existing Analyst Skills

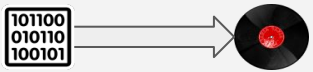
- Create online account for cloud-based service
- Onsite deployment possible

Easy and Safe to Deploy

Benefits - Feedback from Users

- Confidence in safe environment for analysis
  - Do not have to worry about setting up and securing a custom setup
  - Not detonating samples on corporate network
- Deeper knowledge of attacks that other tools don’t provide
  - Often receive alerts that something is bad but don’t know why
  - REnigma provides independent, fast, and deep understanding of attacks
- Actionable information
  - Results from REnigma used immediately to block threats
  - Able to obtain results more quickly than other tools

Competition

Static Analysis ● Requires expensive and highly skilled analyst ● Takes weeks to analyze samples ● Example product: IDA Pro	**REnigma designed to provide answers within minutes** 
Traditional Commercial Sandbox ● Limited to coarse-grained analysis ● Do not support replay ● Example product: Joe's Sandbox (well known)	**REnigma records 100% of activity to dig in deep** 
Custom System (i.e., with open source) ● Requires costly expert for setup/maintenance ● Easy for attackers to study and evade ● Example tool: custom virtual machine	**REnigma easy to configure and leaves nowhere to hide** 

REnigma Summary

- Powerful capability to quickly analyze threats that bypass your defenses
- Takes minutes rather than weeks of analysis
- Results gained from REnigma help keep your network safe

DTRSEC Services

- REnigma for Enterprise IT
  - 4 month trial period
  - Host on site or in DTRSEC Cloud
  - Options for improved performance and reliability
- Malware Analysis Training
  - Operating systems and computer architecture basics
  - Study recordings of real malware in action
  - Learn advanced malware analysis with REnigma

Contact us for more information

Julian Grizzard, Co-Founder
Julian@dtrsec.com
Deterministic Security, LLC

Jim Stevens, Co-Founder
Jim@dtrsec.com
Deterministic Security, LLC