

Rooma Sec

White Paper

Rooma X-WING *AI-native* NG-EDR

Free trial available

Supports public cloud SaaS

Faster security **Boost business**

Covering the MITRE ATT&CK Framework, and coupling cloud-native architecture with kernel-level lightweight sensors, detects stealthy, new types of attacks fastly.

Contact us: support@xrooma.com

Table of Contents

01 What is NG-EDR?

AI Native 1

Detects and Tracks New Attacks Faster 1

02 Benefits of Rooma X-WING NG-EDR 2

Benefit 1: Faster Threat Detection 3

Benefit 2: More rapid Attack Traceback 4

Benefit 3: Quicker Data Collection 5

Benefit 4: Faster Installation and Deployment 6

03 How Does Rooma Achieve This ?

Superior Kernel-Level Lightweight Sensor 7

Powerful Advanced Threat Hunting Capability 7

04 Four Application Scenarios 8

Detects Ransomware Attacks in Depth 9

Uncovers Fileless Attacks Effectively 11

Identifies Phishing Attacks Effectively 13

Spots Mining Attacks Accurately 15

05 Customer Stories

Typical Customer Story 17

06 SaaS Free Trial

How to get a SaaS free trial? 18

01 Introduction of NG-EDR

What is NG-EDR?

Problem with Current EDR: Investigates and Validates New Attacks Slowly.

Reasons for Slowness

- ✗ Incomplete endpoint behavior capture caused by technical issues leading to false negatives in clues.
- ✗ The large number of detections generated by threat behaviors collected make it difficult to get priorities right and require heavy manual involvement which then causes delayed investigation and validation.

How to Speed Up?

Rooma's Definition of NG-EDR

AI Native

- ✓ Based on generative AI, it now can generate attack analysis reports in minutes which otherwise take security experts days to complete.

Detects and Tracks New Attacks Faster

- ✓ Intelligently aggregates threat incidents, correlates a large number of detections to build a knowledge graph, and then condenses them into critical incidents that demand attention from customers, thus allowing faster investigation and validation of new attacks.

Benefits of Rooma X-WING NG-EDR

Traditional endpoint security products
SLOW

VS

Rooma X-WING AI-native NG-EDR
FAST

How quickly to catch new types of attacks?

Threat detection Intelligent technology, detects in minutes!

- ✗ AV
Relies on characteristics such as file HASH for detection, making it difficult to discover new attacks without known patterns.
- ✗ Ordinary EDR
Generates a large number of detections, making it challenging to get priorities straight. It requires both heavy manual involvement and a huge amount of time, leading to slow analysis of attacks.

- ✓ Behavior-based intelligent detection technology can accurately identify attacks even if file characteristics such as HASH keep changing.
- ✓ Intelligent aggregation of threat incident ensures valuable clues are not in floods of alerts, allowing rapid detection of new attacks.

How fast to generate threat report?

Attack traceback Generative AI, instant reporting!

- ✗ It will take experts days to investigate and tracks different security-related events before complete a report.

- ✓ Leverages generative AI, and threat reports can be directly generated or exported from the display showing attack details and contexts.

How rapid does the sensor run?

Data collection Kernel-level lightweight sensor, no system slowdown!

- ✗ CPU usage exceeds 1% or even 10%, and memory usage ranges from tens of megabytes to several hundred megabytes.

- ✓ Typically, endpoint CPU usage is less than 0.1%, and memory usage is under 15M.

How fast is the installation and deployment?

Installation and deployment SaaS deployment, just login and use!

- ✗ Both procurement and installation are complex. It usually takes days or even weeks before users can use the product.

- ✓ Supports public cloud SaaS deployment, allowing users to start using by downloading and installing lightweight sensors from the cloud.

>400

Covers 400+ ATT&CK techniques

>2000

Supports 2000+ detectable attack patterns

<0.1%

typical endpoint CPU usage < 0.1%

<15M

typical endpoint memory usage <15M

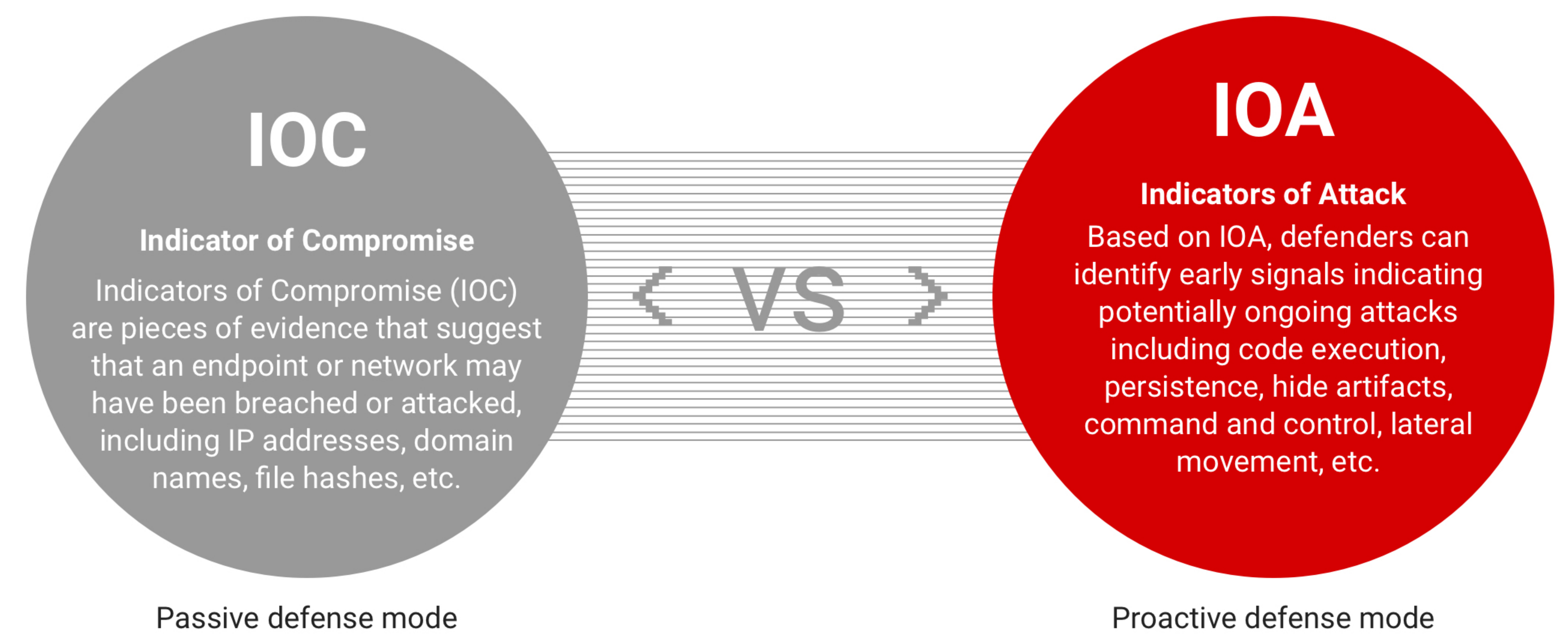
02

Benefits of Rooma X-WING NG-EDR

Benefit 1: Faster Threat Detection

Intelligent technology, detects in minutes!

- Behavior-based intelligent detection technology can accurately identify attacks even if file characteristics such as HASH keep changing.



- Intelligent aggregation of threat incidents ensures valuable clues are not in floods of alerts, allowing rapid detection of new attacks.

| Score | Detections | Host | Time | Ticket |
|-------------------------------|---|---|---|--|
| Critical 10 _{/10} | <div><div>Machine Learning via Sensor-based ML</div><div>Credential Access via OS Credential Dumping</div><div>Other detections & contextual detections</div></div> <div>16 2 8 Total 26</div> | <div>Host name Operating system External IP Connection IP</div> <div>DESKTOP-A4PH56B windows 10 216.285.101 216.285.101</div> | <div>Start Last activity Duration</div> <div>Sep. 12, 2023 15:00:00 Sep. 12, 2023 16:00:00 1h 0m 0s</div> <div></div> | <div>Incident Status</div> <div>DESKTOP-DVKGSD-2024011110 New</div> <div><div>View</div><div>Edit</div><div>AI Report</div></div> |
| High 6.7 _{/10} | <div><div>Machine Learning via Sensor-based ML</div><div>Credential Access via OS Credential Dumping</div><div>Other detections & contextual detections</div></div> <div>8 1 1 Total 10</div> | <div>Host name Operating system External IP Connection IP</div> <div>DESKTOP-A4PH56B windows 10 216.285.101 216.285.101</div> | <div>Start Last activity Duration</div> <div>Sep. 12, 2023 15:00:00 Sep. 12, 2023 16:00:00 1h 0m 0s</div> <div></div> | <div>Incident Status</div> <div>DESKTOP-DVKGSD-2024011110 In Progress</div> <div><div>View</div><div>Edit</div><div>AI Report</div></div> |
| High 6.6 _{/10} | <div><div>Machine Learning via Sensor-based ML</div><div>Credential Access via OS Credential Dumping</div><div>Other detections & contextual detections</div></div> <div>6 10 12 Total 28</div> | <div>Host name Operating system External IP Connection IP</div> <div>DESKTOP-A4PH56B windows 10 216.285.101 216.285.101</div> | <div>Start Last activity Duration</div> <div>Sep. 12, 2023 15:00:00 Sep. 12, 2023 16:00:00 1h 0m 0s</div> <div></div> | <div>Incident Status</div> <div>DESKTOP-DVKGSD-2024011110 Closed</div> <div><div>View</div><div>Edit</div><div>AI Report</div></div> |
| Medium 2.6 _{/10} | <div><div>Machine Learning via Sensor-based ML</div><div>Credential Access via OS Credential Dumping</div><div>Other detections & contextual detections</div></div> <div>5 6 10 Total 21</div> | <div>Host name Operating system External IP Connection IP</div> <div>DESKTOP-A4PH56B windows 10 216.285.101 216.285.101</div> | <div>Start Last activity Duration</div> <div>Sep. 12, 2023 15:00:00 Sep. 12, 2023 16:00:00 1h 0m 0s</div> <div></div> | <div>Incident Status</div> <div>DESKTOP-DVKGSD-2024011110 False Positive</div> <div><div>View</div><div>Edit</div><div>AI Report</div></div> |
| Low 2.3 _{/10} | <div><div>Machine Learning via Sensor-based ML</div><div>Credential Access via OS Credential Dumping</div><div>Other detections & contextual detections</div></div> <div>16 2 8 Total 26</div> | <div>Host name Operating system External IP Connection IP</div> <div>DESKTOP-A4PH56B windows 10 216.285.101 216.285.101</div> | <div>Start Last activity Duration</div> <div>Sep. 12, 2023 15:00:00 Sep. 12, 2023 16:00:00 1h 0m 0s</div> <div></div> | <div>Incident Status</div> <div>DESKTOP-DVKGSD-2024011110 False Positive</div> <div><div>View</div><div>Edit</div><div>AI Report</div></div> |
| Low 1.2 _{/10} | <div><div>Machine Learning via Sensor-based ML</div><div>Credential Access via OS Credential Dumping</div><div>Other detections & contextual detections</div></div> <div>12 2 6 Total 20</div> | <div>Host name Operating system External IP Connection IP</div> <div>DESKTOP-A4PH56B windows 10 216.285.101 216.285.101</div> | <div>Start Last activity Duration</div> <div>Sep. 12, 2023 15:00:00 Sep. 12, 2023 16:00:00 1h 0m 0s</div> <div></div> | <div>Incident Status</div> <div>DESKTOP-DVKGSD-2024011110 False Positive</div> <div><div>View</div><div>Edit</div><div>AI Report</div></div> |
| Low 1.1 _{/10} | <div><div>Machine Learning via Sensor-based ML</div><div>Credential Access via OS Credential Dumping</div><div>Other detections & contextual detections</div></div> <div>16 2 8 Total 26</div> | <div>Host name Operating system External IP Connection IP</div> <div>DESKTOP-A4PH56B windows 10 216.285.101 216.285.101</div> | <div>Start Last activity Duration</div> <div>Sep. 12, 2023 15:00:00 Sep. 12, 2023 16:00:00 1h 0m 0s</div> <div></div> | <div>Incident Status</div> <div>DESKTOP-DVKGSD-2024011110 False Positive</div> <div><div>View</div><div>Edit</div><div>AI Report</div></div> |

02

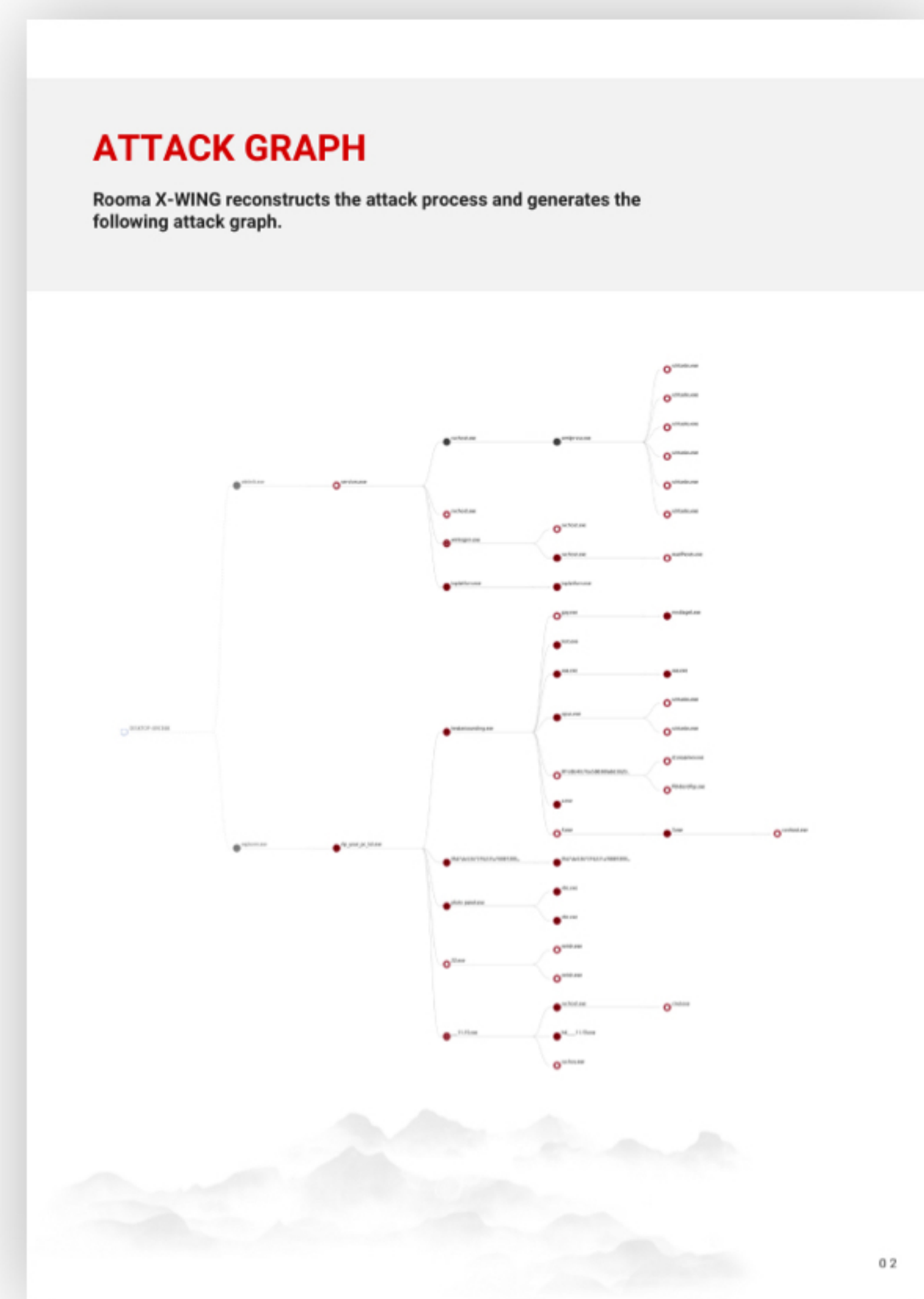
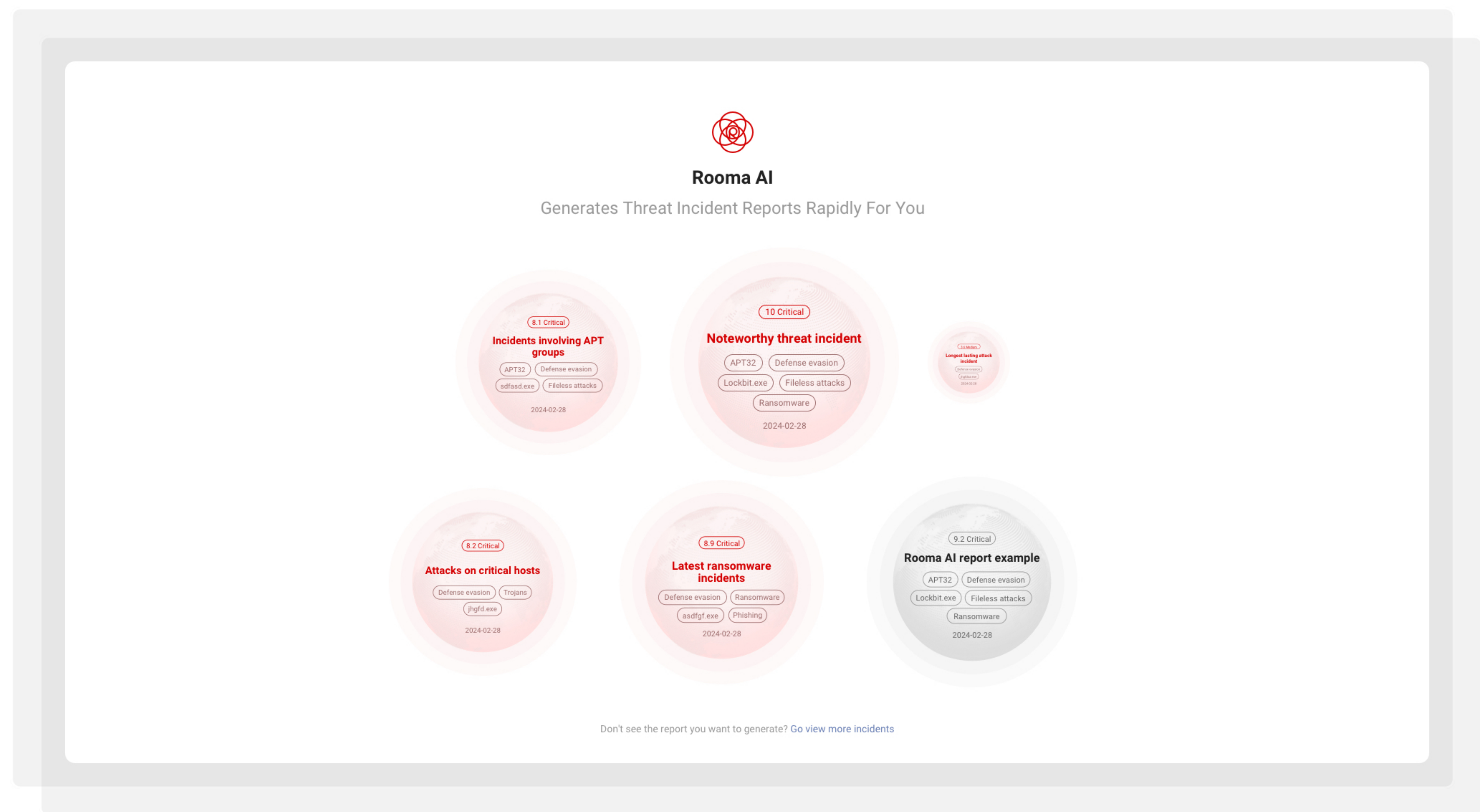
Benefits of Rooma X-WING NG-EDR

Benefit 2: More rapid Attack Traceback

Generative AI, instant reporting!

- ✓

Leverages generative AI, and threat reports can be directly generated or exported from the display showing attack details and contexts.




02

Benefits of Rooma X-WING NG-EDR

Benefit 3: Quicker Data Collection

Kernel-level lightweight sensor

- ✓
- Because more than 80% of data is collected through the Windows kernel, so the sensor is lightweight which consumes fewer resources of the endpoint than other similar products.

| Core index | |  Rooma X-WING | CrowdStrike | Microsoft ATP | An EDR enterprise in China | Sysmon |
|------------------------------|----------------------------|--|-------------|---------------|----------------------------|--------|
| Event collection capability | ATT&CK DataSource coverage | >100% | 100% | 100% | 90% | 10% |
| | Event type | 48 | 46 | 21 | 40+ | 27 |
| | Event number | 500 | 482 | - | 90+ | 27 |
| Sensor Resources Consumption | -CPU usage | <0.1% | <1% | 1% | 5% | 0.3% |
| | -Memory usage | <15M | 227M | 70M | 30M | 15M |

Data source: public materials or measured data

What is Kernel-level Data Collection?

Windows Kernel-level data collection is an advanced technology that allows developers or system administrators to monitor and collect various system information within the operating system kernel including process and thread, memory usage, network traffic, file system operations, etc. Kernel-level data collection finds widespread application in areas such as system management, performance optimization, and security analysis.

Why is Kernel-level Data Collection superior?

Through kernel-level data collection, it is possible to acquire the lower-level and more comprehensive system information, not limited to data visible in the user space. This is particularly useful for system performance analysis, security monitoring, and troubleshooting. Moreover, compared to user-mode data collection, kernel-level data collection is faster and consumes less endpoint resources.

Why can Rooma make it?

The Rooma X-WING R&D team is highly professional, with both profound academic background and theoretical knowledge, as well as many years of rich experience in kernel-level data collection. This team of experts continues to make technical breakthroughs in the field of endpoint data collection, helping users efficiently deal with increasingly severe security challenges.

Benefit 4: Faster Installation and Deployment

SaaS deployment, just login and use!

- ✓ Supports public cloud SaaS deployment, allowing users to start using by downloading and installing lightweight sensors from the cloud.

Provides SaaS Offering

Cloud-Native Architecture, Deployment in minutes, ready to use instantly, and convenient for expanding endpoint amounts and time dynamically.


Kernel-level lightweight sensor, no system slowdown

Supports unified silent installation by administrators, kernel-level lightweight sensor without system slowdown.

Cloud-based Expert Real-time Threat Hunting

Notifies customers in time and assists to resolve urgent threats once uncovered.

In-depth Analysis of Threat Behavior


In-depth analysis of massive
endpoint behavior logs



AI-based intelligent analysis



Cloud-based expert threat hunting



Endpoint Behavior Log Collection


User endpoint deployed
with Rooma X-WING sensor



User endpoint



User endpoint



User endpoint

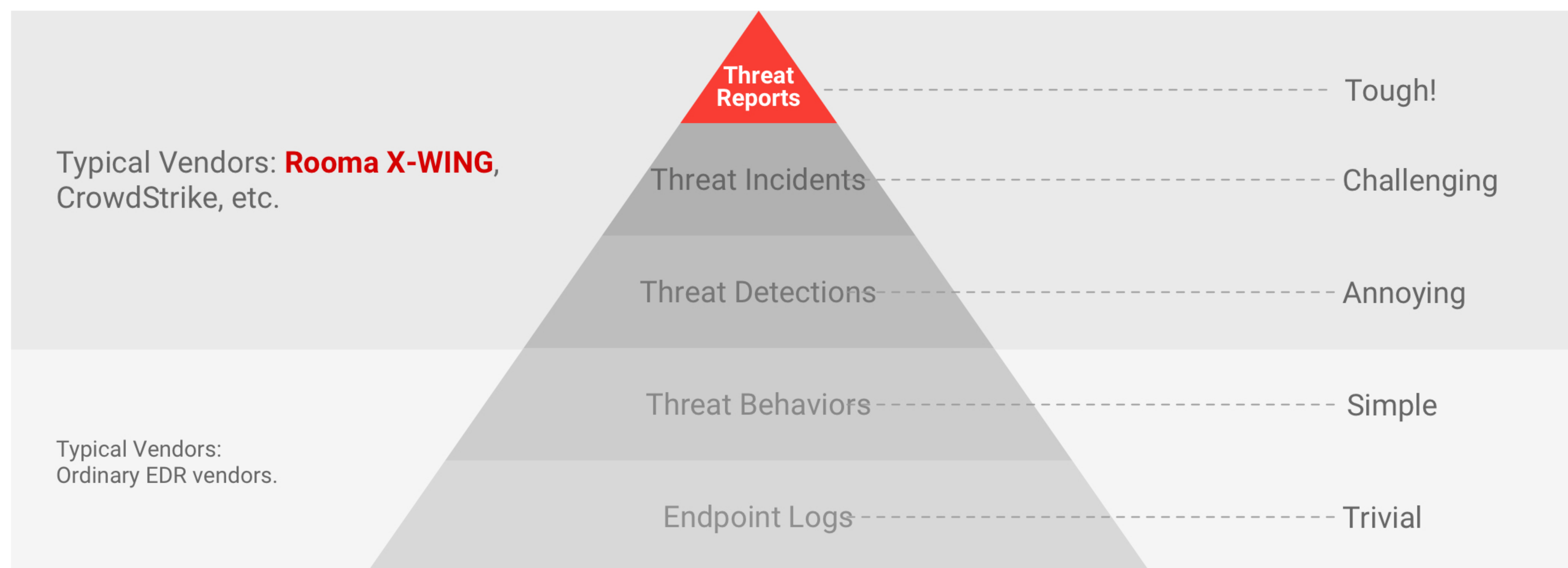
How Does Rooma Achieve This?

Superior Kernel-Level Lightweight Sensor

- ✓ Leverages kernel-level data collection technology, collecting endpoint behavior logs and ensuring no system slowdown.

Powerful Advanced Threat Hunting Capability

- ✓ Based on massive logs, efficiently and intelligently detects threat incidents using Rooma's distinctive algorithms and rapidly generates threat reports restoring the attack process, which saves time and effort.



Pyramid of Advanced Threat Insight

Typical Application Scenarios and Use Cases

Detects ransomware attacks in depth

- ✓ In-depth detection based on threat behavior and data recovery guarantee provide dual protection.

Uncovers fileless attacks effectively

- ✓ Combining static memory detection and dynamic behavior monitoring, makes fileless attacks have nowhere to hide.

Identifies phishing attacks effectively

- ✓ Coupling static characteristics with dynamic behavior tracking, ensures no new bait is missed.

Spots Mining Attacks accurately

- ✓ Focusing on threat behaviors, accurately discovers mining pools and machines, not afraid of mining attacks.

Detects **Ransomware** Attacks in Depth

Ransomware attacks on the rise

In recent years, ransomware has become one of the most devastating types of malware, with hackers making huge profits by encrypting the victims' important files and then demanding a ransom. RaaS (Ransomware as a Service) has quietly become a dark industry chain, and more and more organizations and individuals have become targets for hackers. Hackers continue to improve their attack techniques and transform file characteristics to evade the static detection mode that traditional endpoint security products rely on.



Rooma X-WING Solution

Traditional endpoint security products are prone to false negatives.

New types of ransomware are emerging one after another. Traditional endpoint security software based on static characteristics detection is prone to false negatives. Only advanced threat detection systems based on threat behavior can solve this problem.

VS

Rooma X-WING endpoint security product provides dual protection, and it is more secure.

- ✓ It can detect in depth and defend against dozens of widespread ransomware, such as Lockbit, WastedLocker and WannaCry;
- ✓ AI-based intelligent threat behavior detection, covering ATT&CK, monitors anomalous behavior in real time to detect in depth and stop ransomware from running;
- ✓ Fully recovers the encrypted files with file rollback technology.

01 See: Dynamic Behavior Detection

- ✓ AI-based intelligent threat behavior identification, covering ATT&CK framework, detects highly stealthy advanced ransomware effectively.
- ✓ Collects full process context, focuses on dynamic and abnormal behaviors, and accurately identifies even mutated and unknown ransomware.
- ✓ Identifies fileless attacks effectively, ensuring advanced fileless ransomware nowhere to hide.

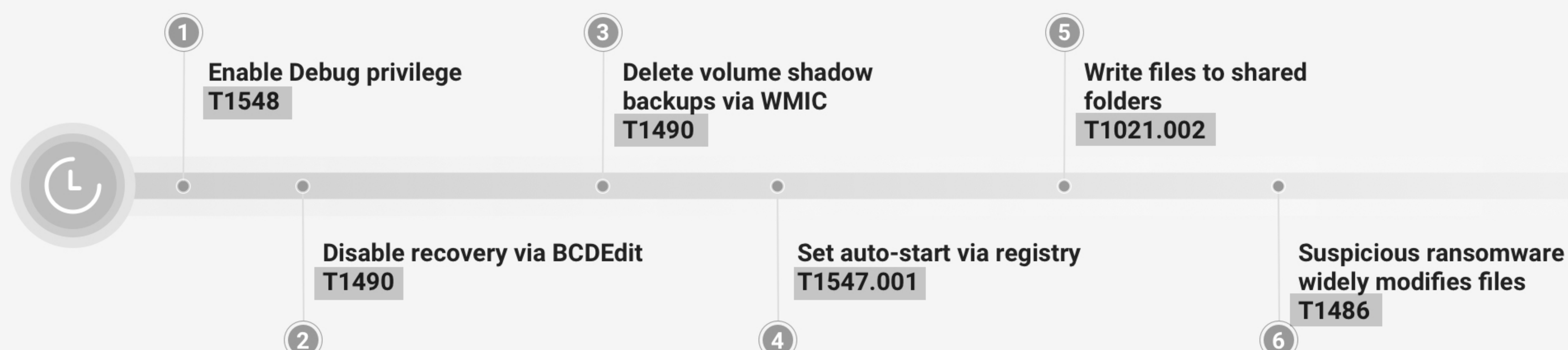
02 Intercept: Ransomware Execution Prevention

- ✓ Stops malicious behaviors of ransomware in real time, preventing data from being encrypted.
- ✓ Blocks known ransomware with high prevalence from running immediately leveraging massive cloud malicious characteristic indicators.
- ✓ Prevents malicious process from creating, and thus stops ransomware from executing fundamentally.

03 Recover: Data Recovery Guarantee

- ✓ Comprehensive defense against ransomware and data recovery guarantee provide dual protection.
- ✓ File rollback technique and memory key extraction technique serve as a safety net, rolling back files being blackmailed and protecting critical data.

LockBit is a new type of ransomware that is extremely harmful. It has reached version 3.0. The ransomware uses multi-threaded encryption, so it encrypts files very quickly, and the encryption mode is one key per file, which can destroy the system restore function and make it difficult to recover from a successful attack.



04

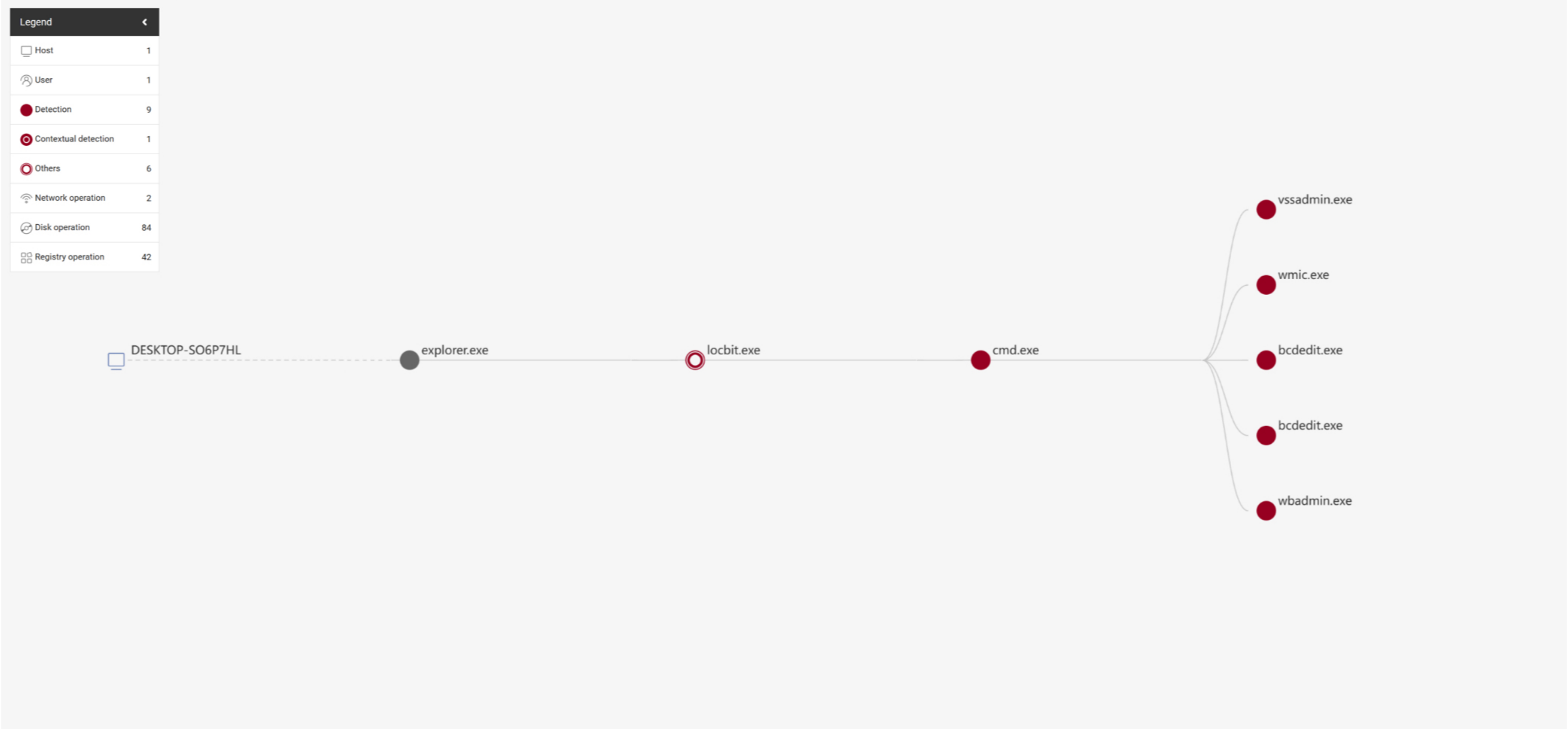
Typical Use Cases

Detects ransomware attacks in depth

Overview of Threat Incidents

| Score | Detection | Host | Timeline | Ticket |
|----------|---|---|---|---|
| Critical | <div><div></div> Impact via Inhibit System Recovery9</div> <div><div></div> Lateral Movement via SMB/Windows Admin Shares1</div> <div><div></div> Other detections & contextual detections6</div> <div>16 total</div> | Host nameDESKTOP-SO6P7HL Operating systemWindows 10 build 19045 External IP192.168.111.78 Connection IP192.168.156.187 | StartFeb. 28,2024 18:43:24 Last activityFeb. 28,2024 18:46:17 Duration0h 2m 53s | IncidentDESKTOP-SO6P7HL-2024022818 Status <div>New</div> <div>View</div> <div>Edit</div> |

Threat Incident Graph



ATT&CK Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|----------------|--|--|--|---|-------------------|---|--|------------|---------------------|--------------|---|
| | <div>T1204: User Execution</div> <div>T1204.002: Malicious File</div> <div>T1106: Native API</div> | <div>T1547: Boot or Logon Autostart Execution</div> <div>T1547.001: Registry Run Keys / Startup Folder</div> | <div>T1547: Boot or Logon Autostart Execution</div> <div>T1547.001: Registry Run Keys / Startup Folder</div> <div>T1548: Abuse Elevation Control Mechanism</div> | <div>T1497: Virtualization/Sandbox Evasion</div> <div>T1497.003: Time Based Evasion</div> <div>T1548: Abuse Elevation Control Mechanism</div> | | <div>T1497: Virtualization/Sandbox Evasion</div> <div>T1497.003: Time Based Evasion</div> <div>T1057: Process Discovery</div> | <div>T1021: Remote Services</div> <div>T1021.002: SMB/Windows Admin Shares</div> | | | | <div>T1490: Inhibit System Recovery</div> <div>T1486: Data Encrypted for Impact</div> |

Uncovers **Fileless** Attacks Effectively

Fileless attacks with a very high probability of successful intrusion

A fileless attack is a new type of attack that involves not writing an executable file to a hard drive. Attackers exploit system or application vulnerabilities, steal passwords or employ other methods to gain access. After gaining access, they leverage the tools or mechanisms that come with the operating system, such as PowerShell, PsExec, WMI, registry, MBR, etc., for deeper penetration and persistence. Since there are no files on disk, this special attack method is particularly easy to evade the detection of traditional endpoint security products, and is a new attack method favored by hackers, and the probability of successful intrusion is very high.



Rooma X-WING Solution

Traditional endpoint security products are hard to detect fileless attacks.

Unlike most malware, fileless attacks leave no trail on hard drive, and it is difficult for traditional file-scanning-based antivirus software to spot because there are no virus files.

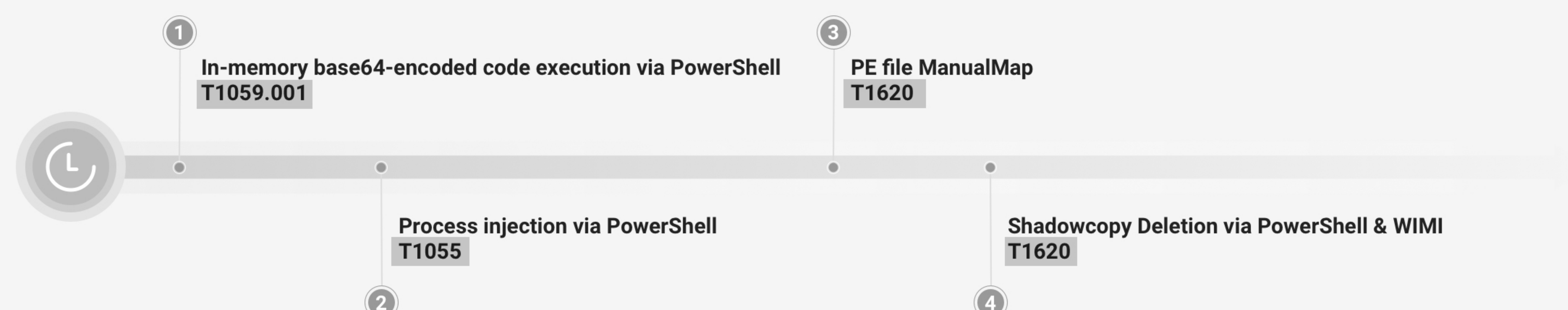
VS

Rooma X-WING utilizes AI-based intelligent threat behavior monitoring.

- ✓ Focusing on suspicious activities (such as code execution, attempts to hide artifacts, lateral movement, etc.) makes it difficult to evade detection, whether booted from a file or from memory;
- ✓ Focusing on process context and behavior sequences effectively detects even malicious behavior with legitimate accounts (often stolen credentials) ;
- ✓ Even malicious codes written by legitimate tools such as PowerShell and obfuscated (encrypted) can be identified accurately.



By abusing the legitimate Windows system tool PowerShell to execute malicious code in memory without touching disk during the procedures, thus evade the detection mechanisms of traditional endpoint security products reliant on static signatures and file characteristics scanning.



04

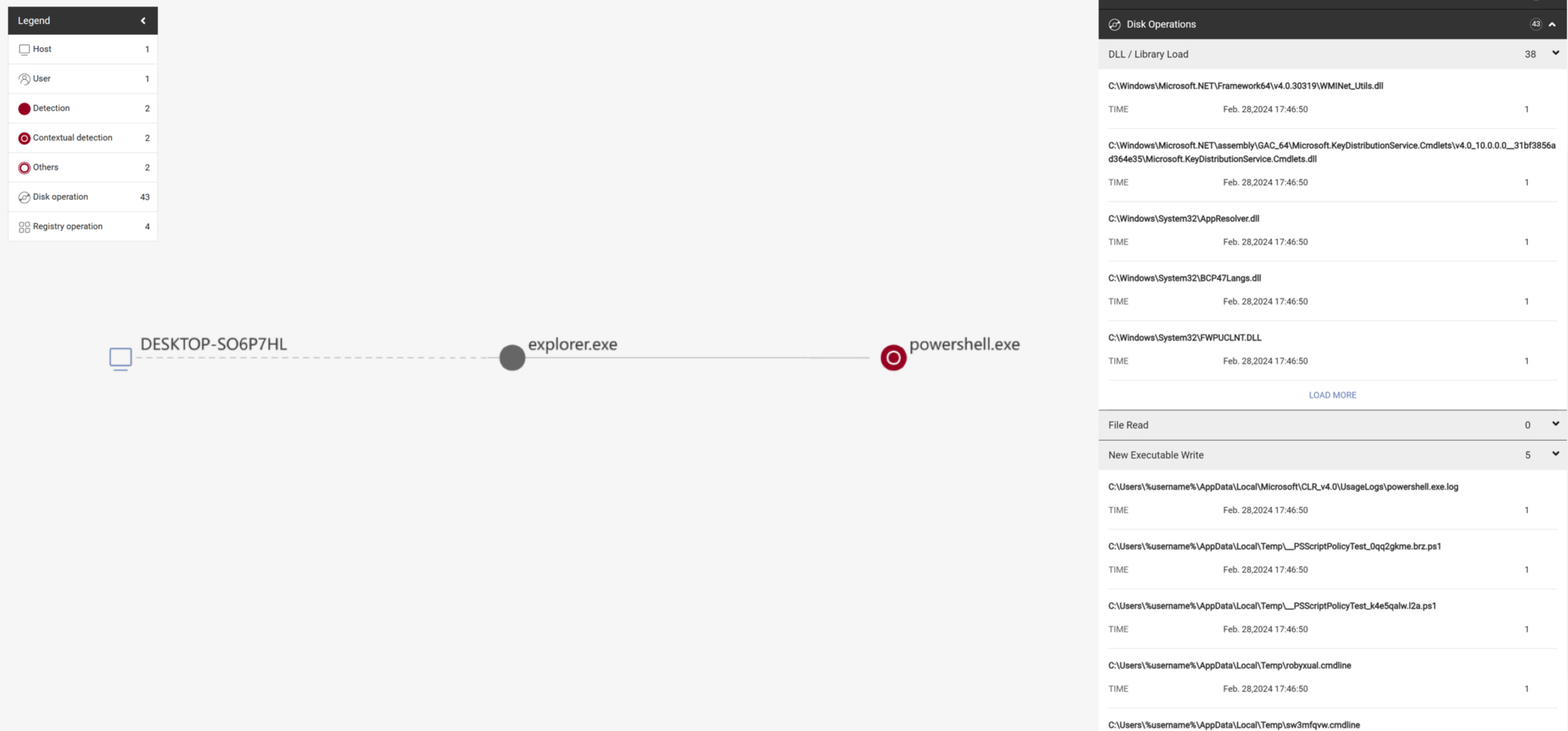
Typical Use Cases

Uncovers **fileless** attacks effectively

Overview of Threat Incidents

| | Score | Detection | Host | Timeline | Ticket |
|----------|---------|---|--|---|--|
| Critical | 9.6 /10 | <div><div>● Impact via Inhibit System Recovery13</div><div>● Defense Evasion via Compile After Delivery2</div><div>● Other detections & contextual detections2</div><div>17 total</div></div> | <div>Host nameDESKTOP-SO6P7HL</div> <div>Operating systemWindows 10 build 19045</div> <div>External IP192.168.111.78</div> <div>Connection IP192.168.156.199</div> | <div>StartFeb. 26,2024 15:44:53</div> <div>Last activityFeb. 26,2024 15:44:53</div> <div>Duration0h 0m 1s</div> | <div>Incident</div> <div>Status</div> <div>FilelessAttack</div> <div>In Progress</div> <div>ViewEdit</div> |

Threat Incident Graph



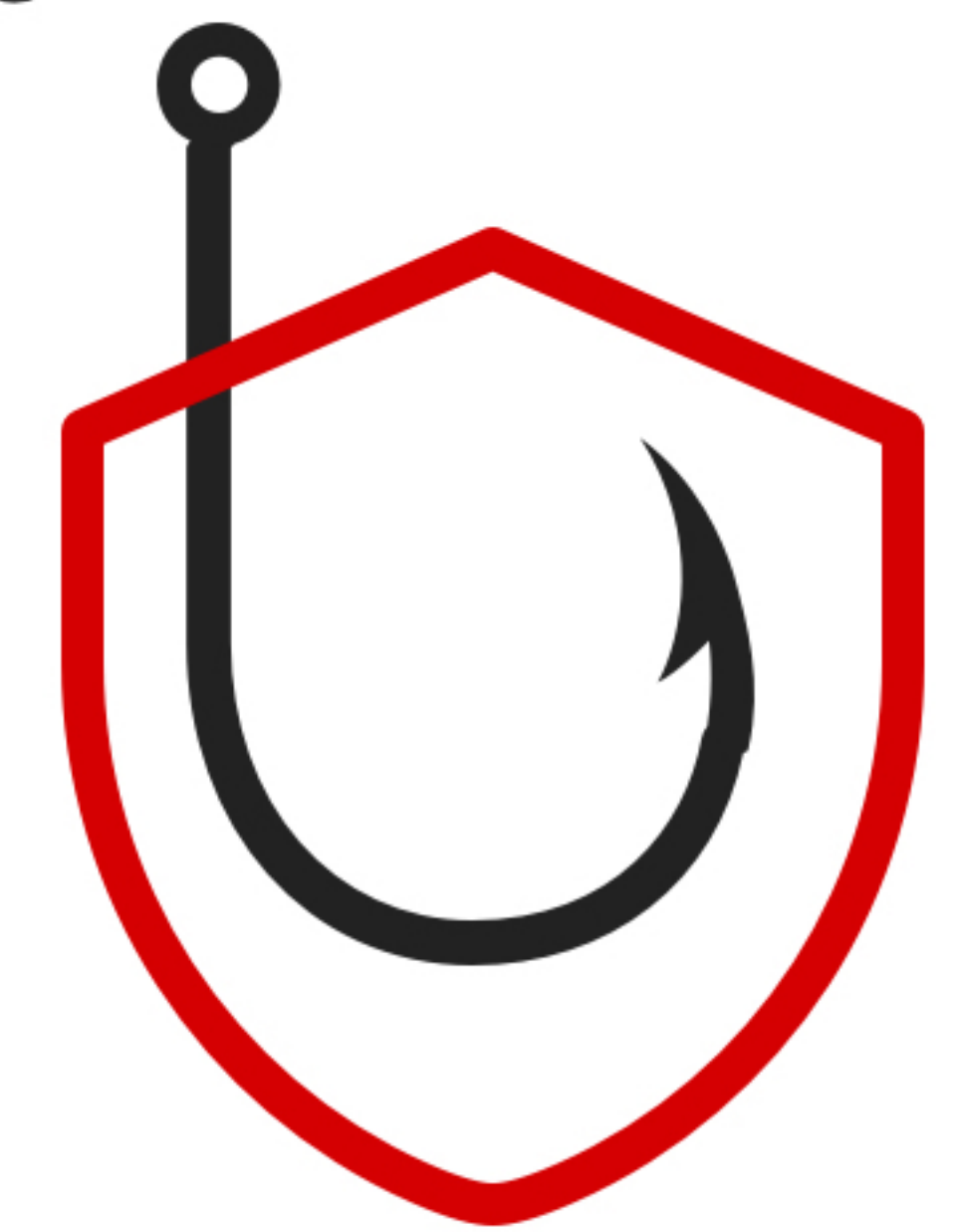
ATT&CK Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|----------------|--|-------------|-------------------------------------|---|-------------------|-----------|------------------|------------|---------------------|--------------|---|
| | <div>T1059: Command and Scripting Interpreter</div> <div>T1059.001: PowerShell</div> | | <div>T1055: Process Injection</div> | <div>T1620: Reflective Code Loading</div> <div>T1055: Process Injection</div> | | | | | | | <div>T1490: Inhibit System Recovery</div> |

Identifies **Phishing** Attacks Effectively

Phishing has become one of the most popular attack techniques

Phishing attacks trick victims into clicking on malicious links or downloading malware for the purpose of information theft, spreading malware, or cyber fraud. Hackers usually send "bait" via email, SMS, or instant messengers to lure clicks, and they carefully craft the bait to try to entice the victim to click. Although phishing attacks have been around for a long time, they are often used by hackers as an entry point to compromise organizations due to their low cost and high benefits. Due to the lack of employee security awareness and the continuous updating of "bait", organizations have a high probability of damage and the rapid spread of infection. It has become a headache for organizational security administrators.



Rooma X-WING Solution

Traditional endpoint security products are prone to false negatives.

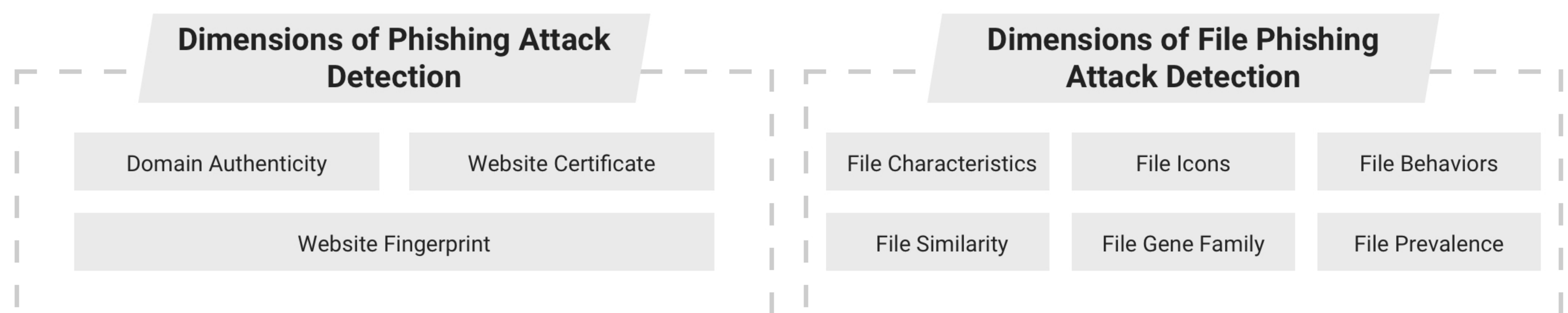
Because hackers often change their "bait", traditional endpoint security products based on static characteristics are prone to false negatives, which may lead to risks such as theft of critical information and rapid malware propagation.

VS

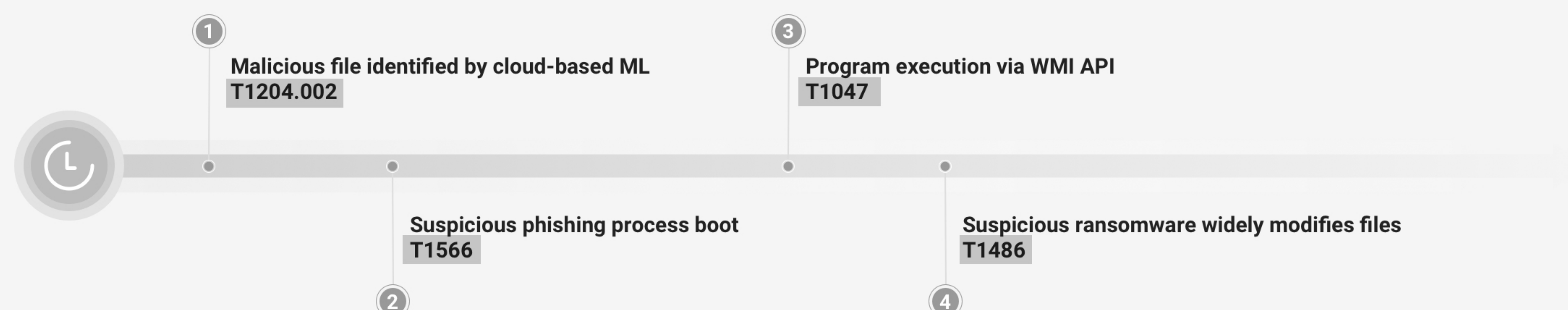
Rooma X-WING the two-pronged detection of characteristics and behaviors can effectively detect phishing attacks

- ✓ Phishing attack detection based on static characteristics;
- ✓ Dynamic behavior monitoring, timely alert once suspicious behavior is identified.

Based on ATT&CK and proprietary phishing detection model, combining static characteristics and dynamic behavior tracking, detects phishing attacks effectively.



Trick users into carefully crafted "bait" and send malware to victims as "detection-free" documents to lure them to click or share them, thus evade static characteristic-based detection by traditional endpoint security products.



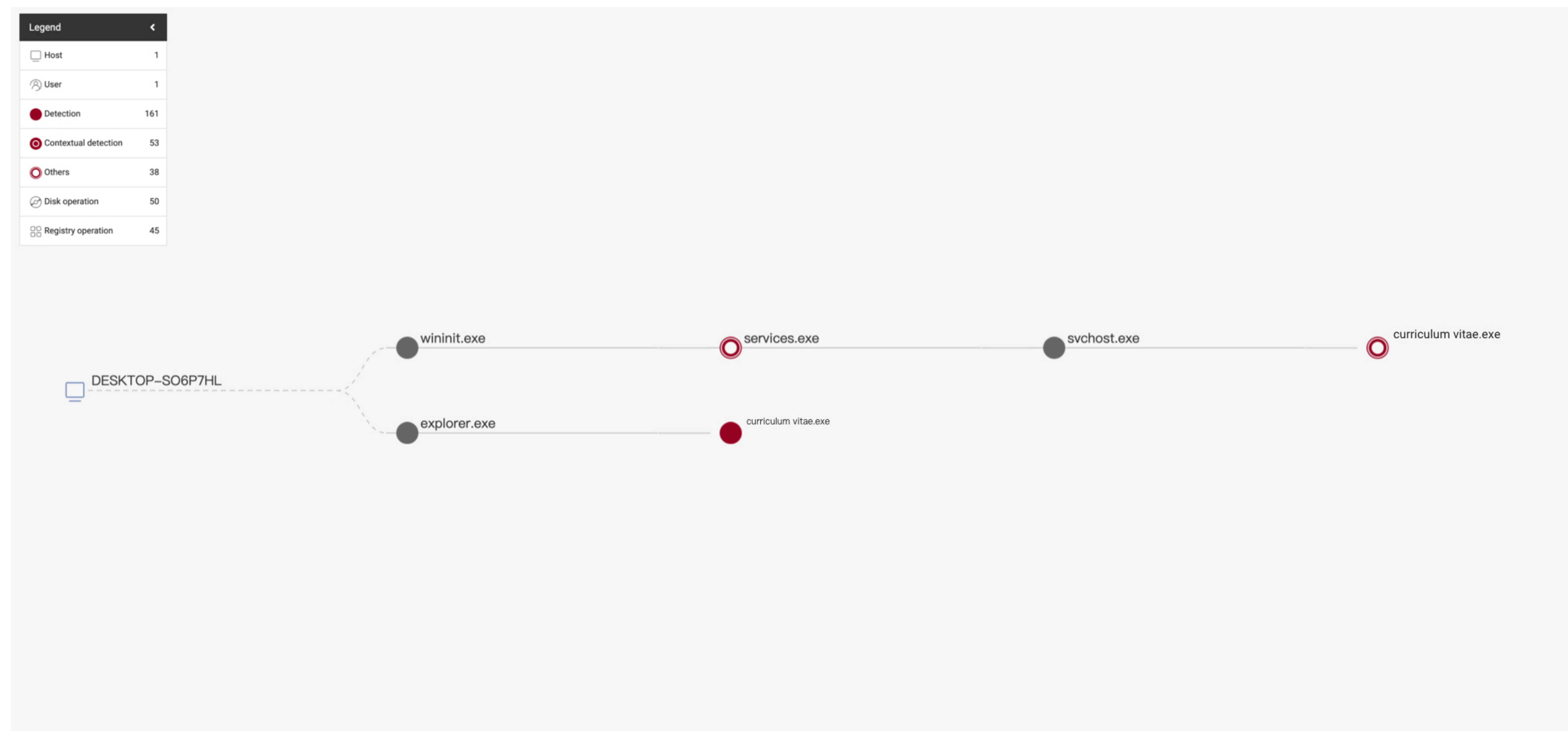
04 Typical Use Cases

Identifies **Phishing** Attacks Effectively

Overview of Threat Incidents

| Score | Detection | Host | Timeline | Ticket |
|---------------------|---|--|--|--|
| Critical 8.7 /10 | <div><div>● Privilege Escalation via Bypass User Account Control4</div><div>● Lateral Movement via SMB/Windows Admin Shares2</div><div>● Other detections & contextual detections9</div><div>15 total</div></div> | <div><div>Host nameDESKTOP-S06P7HL</div><div>Operating systemWindows 10 build 19045</div><div>External IP192.168.111.78</div><div>Connection IP192.168.156.211</div></div> | <div><div>StartFeb. 26,2024 16:48:38</div><div>Last activityFeb. 26,2024 16:52:46</div><div>Duration0h 4m 8s</div></div> | <div><div>IncidentDESKTOP-S06P7HL-2024022616</div><div>StatusIn Progress</div><div>View Edit</div></div> |

Threat Incident Graph



ATT&CK Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|--------------------------------|---|--|--|---|-------------------|---|--|------------|---------------------|---|--------|
| <div>T1566: Phishing</div> | <div>T1204: User Execution</div> <div>T1204.002: Malicious File</div> | <div>T1547: Boot or Logon Autostart Execution</div> <div>T1547.001: Registry Run Keys / Startup Folder</div> <div>T1547.009: Shortcut Modification</div> | <div>T1548: Abuse Elevation Control Mechanism</div> <div>T1548.002: Bypass User Account Control</div> <div>T1547: Boot or Logon Autostart Execution</div> <div>T1547.001: Registry Run Keys / Startup Folder</div> <div>T1547.009: Shortcut Modification</div> | <div>T1548: Abuse Elevation Control Mechanism</div> <div>T1548.002: Bypass User Account Control</div> <div>T1112: Modify Registry</div> | | <div>T1057: Process Discovery</div> | <div>T1021: Remote Services</div> <div>T1021.002: SMB/Windows Admin Shares</div> | | | <div>T1486: Data Encrypted for Impact</div> <div>T1486: Data Encrypted for Impact</div> | |

04 Typical Use Cases

Spots Mining Attacks Accurately

Mining attacks cause legal risk

Mining attacks refer to attackers' attempts to implant cryptomining malware into the victim's computer, and secretly mine cryptocurrency on the victim's device without his/her knowledge or consent. This can lead to a slower computer, a lot of energy consumption, a reduced hardware lifespan, and even legal risks.



Rooma X-WING Solution

Traditional endpoint security products are prone to false negatives.

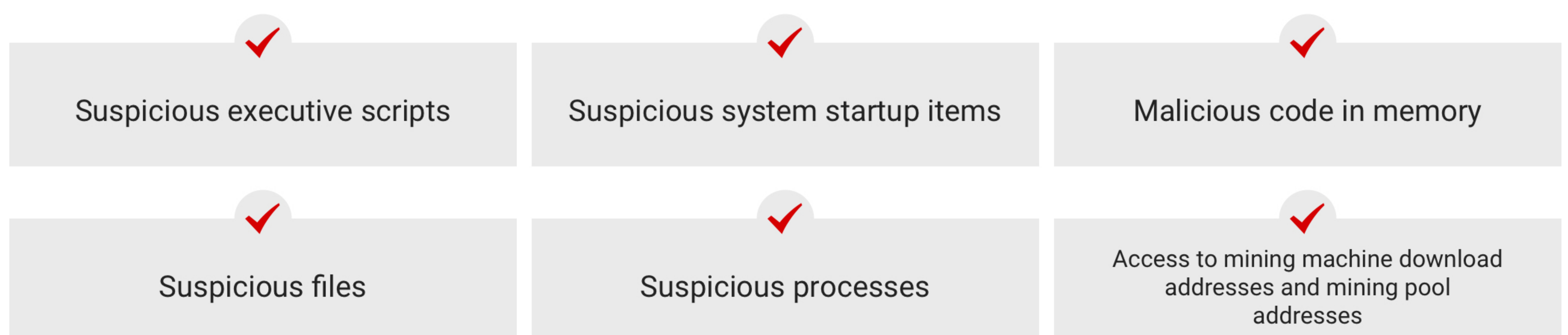
Traditional endpoint security products are ineffective against new and covert mining malware, and cannot effectively prevent mining attacks via phishing.

VS

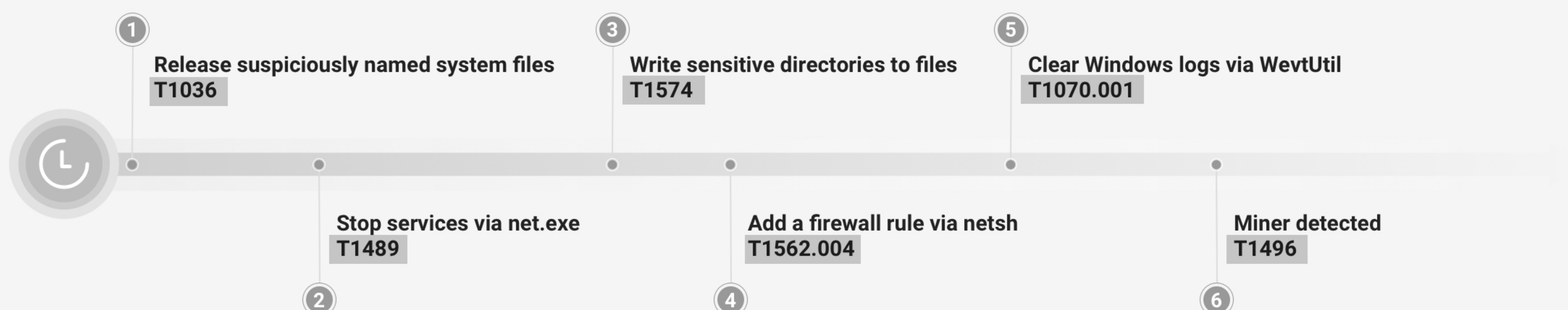
Rooma X-WING relies on behavior-based detection, unafraid to mining attacks.

- ✓ Based on the analysis of endpoint behavior, identifies suspicious computer activities (such as connecting to mining pools, accessing to mining machine download addresses, etc.), and quickly detects mining attacks;
- ✓ By capturing abnormal behavior, new mining attacks can be spotted in time.

Multi-anchor detection of mining attacks based on threat behavior



Being infected by mining viruses often have no obvious characteristics, so it is easy to evade the static characteristics-based detection of traditional products. Attackers implant 'miner' software into the computer and use persistent attack techniques to lurk in the host for a long time, leverage the compromised resources to perform virtual currency calculations, and continuously connect to the "mining pool" for illegal mining activities.

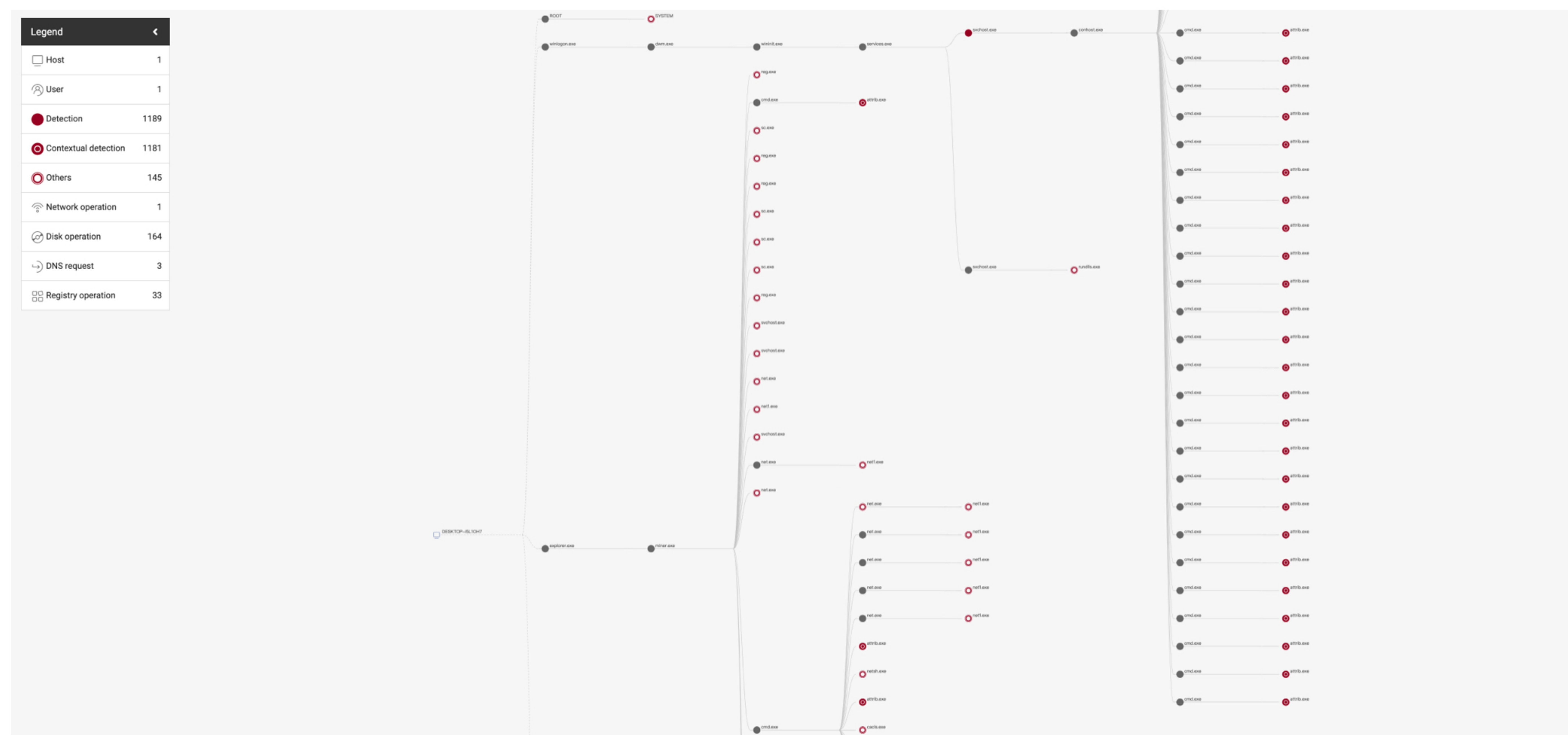


04 Typical Use Cases

Overview of Threat Incidents

| Score | Detection | Host | Timeline | Ticket |
|---|--|------------------|------------------------|--|
| <div>Critical</div> <div>9.7</div> <div>/10</div> | <div><div></div>Defense Evasion via Hida Artifacts</div> <div>666</div> | Host name | DESKTOP-ISL1QH7 | <div>Incident</div> <div>Status</div> <div>MiningAttack</div> <div>In Progress</div> <div><div>View</div><div>Edit</div></div> |
| | <div><div></div>Defense Evasion via File and Directory Permissions M...</div> <div>657</div> | Operating system | Windows 10 build 19043 | |
| | <div><div></div>Other detections & contextual detections</div> <div>145</div> | External IP | 192.168.111.144 | |
| | <div>1468 total</div> | Connection IP | 192.168.23.128 | |
| | | | | |

Threat Incident Graph



ATT&CK Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|----------------|---|--|--|---|--|----------------------------|------------------|------------|---------------------|--------------|------------------------------|
| | T1059: Command and Scripting Interpreter | T1546: Event Triggered Execution | T1546: Event Triggered Execution | T1036: Masquerading | T1555: Credentials from Password Stores | T1622: Debugger Evasion | | | | | T1489: Service Stop |
| | T1106: Native API | T1546.012: Image File Execution Options Injection | T1546.012: Image File Execution Options Injection | T1564: Hide Artifacts T1564.001: Hidden Files and Directories | | | | | | | T1496: Resource Hijacking |
| | T1204: User Execution | T1547: Boot or Logon Autostart Execution | T1547: Boot or Logon Autostart Execution | T1218: System Binary Proxy Execution | | | | | | | |
| | T1204.002: Malicious File | T1547.009: Shortcut Modification | T1547.009: Shortcut Modification | | | | | | | | |
| | | T1574: Hijack Execution Flow | T1574: Hijack Execution Flow | T1562: Impair Defenses | | | | | | | |
| | | | | T1562.004: Disable or Modify System Firewall | | | | | | | |
| | | T1543: Create or Modify System Process | T1543: Create or Modify System Process | T1574: Hijack Execution Flow | | | | | | | |
| | | T1543.003: Windows Service | T1543.003: Windows Service | T1014: Rootkit | | | | | | | |
| | | | | T1070: Indicator Removal on Host | | | | | | | |
| | | | | T1070.001: Clear Windows Event Logs | | | | | | | |
| | | | | T1222: File and Directory Permissions Modification | | | | | | | |

A Typical Customer Story

The World's Leading Enterprises Trust Rooma

- ✓ Rooma X-WING has been deployed in the office network of a leading enterprise in China, running stably on over 10,000 endpoints for more than 500 days.

In
minutes

FastFaster threat detection

Behavior-based threat detection has repeatedly identified threats such as memory-resident malware and fileless attacks in real user environments that were difficult to detect.

>10,000

Number of sensors deployed

Rooma X-WING has been deployed in the office network of a leading enterprise in China and has timely identified threats for the user several times, running stably on over 10,000 endpoints for more than 500 days.

>500

Days of stable operation

Since the deployment of Rooma X-WING on the user's office network, all hosts have been running stably for over 500 days without any product failures.

<0.1%

Endpoint CPU usage

We have calculated resource usage of Rooma X-WING on user hosts, and found the CPU usage is extremely low, not exceeding 0.1% generally, which is significantly lower than that of the user's previous endpoint security agent.

<15M

Endpoint memory usage

We have calculated resource usage of Rooma X-WING on user hosts, and found the memory usage is extremely low, not exceeding 15M generally, which is significantly lower than that of the user's previous endpoint security agent.

How to get a SaaS free trial?

Experience faster threat detection in minutes with no hardware investment.

01

Visit Rooma official website xrooma.com

02

Sign up using email address

03

Click 'Start Free Trial', and get access to Rooma X-WING after approval.

04

Experience the AI-native NG-EDR on Rooma X-WING product interface.

Rooma X-WING **AI-native** NG-EDR

Faster security, Boost business

Covering the MITRE ATT&CK Framework, and coupling cloud-native architecture with kernel-level lightweight sensors, detects stealthy, new types of attacks fastly.

About Rooma

Established in 2021, the founding team members of Rooma Technology (Beijing) Co., Ltd. come from well-known security companies and have more than ten years of experience in the cybersecurity industry. Rooma, takes the actual combat effect of offense and defense as the gold standard for evaluating products, and is committed to solving the problem of undetectable and slow detection of advanced threats in the industry. The self-developed Rooma X-WING AI-native NG-EDR adopts a cloud-native architecture, equipped with a kernel-level lightweight sensor, and the intelligent threat behavior detection mode covers the ATT&CK security framework, which can quickly identify advanced, complex, and new attacks with strong concealment. Leveraging generative AI, X-WING can quickly output attack analysis and traceability reports, saving users valuable time to focus on their business.

✉ support@xrooma.com

For a free trial, please visit xrooma.com ©2024 Rooma Sec. All Rights Reserved.