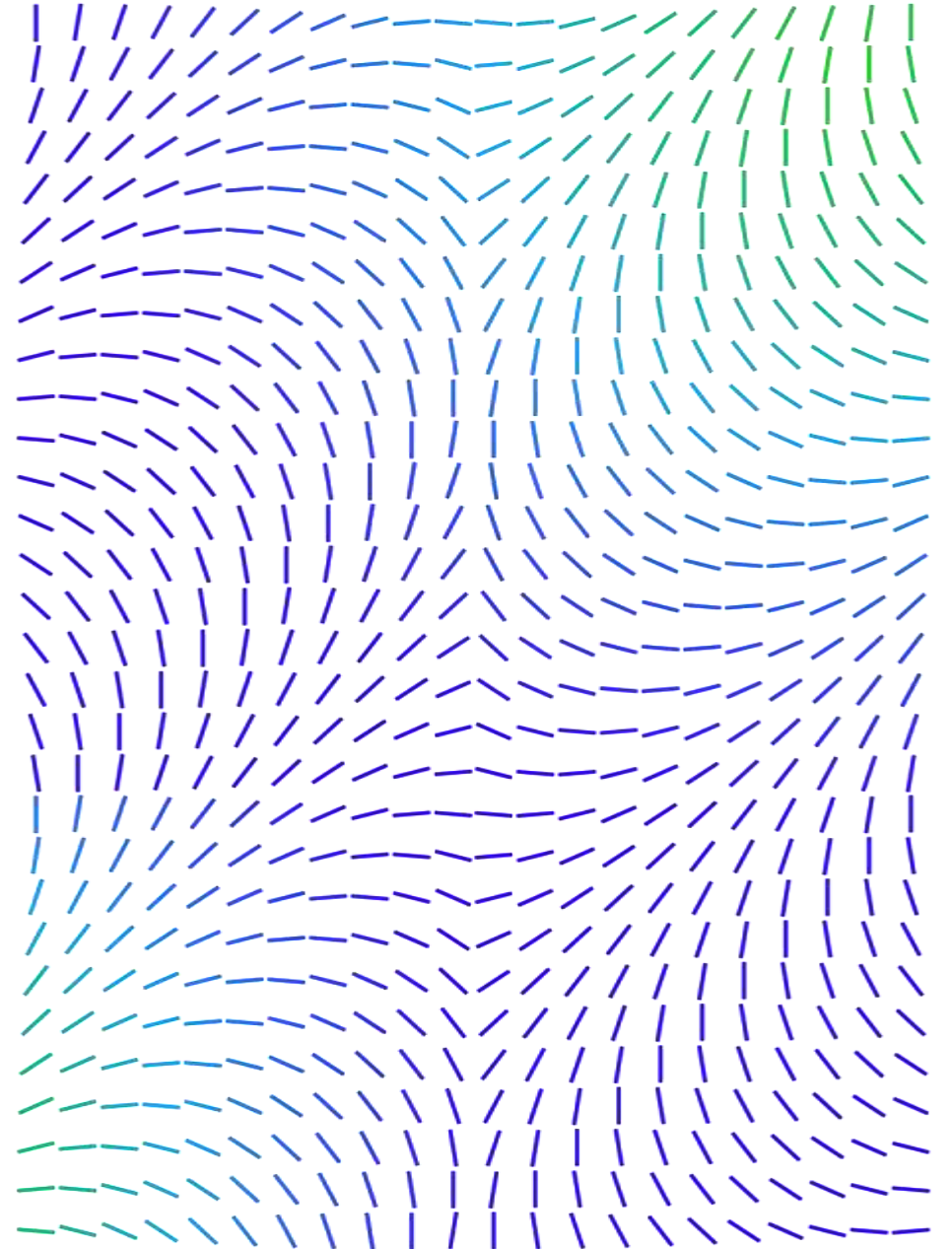




# Trellix XDR Platform



# Trellix?



# Challenges in Security Operations

70

Average number of security tools

10k

Number of security alerts daily

30<sub>min</sub>

Time required to triage  
a single alert

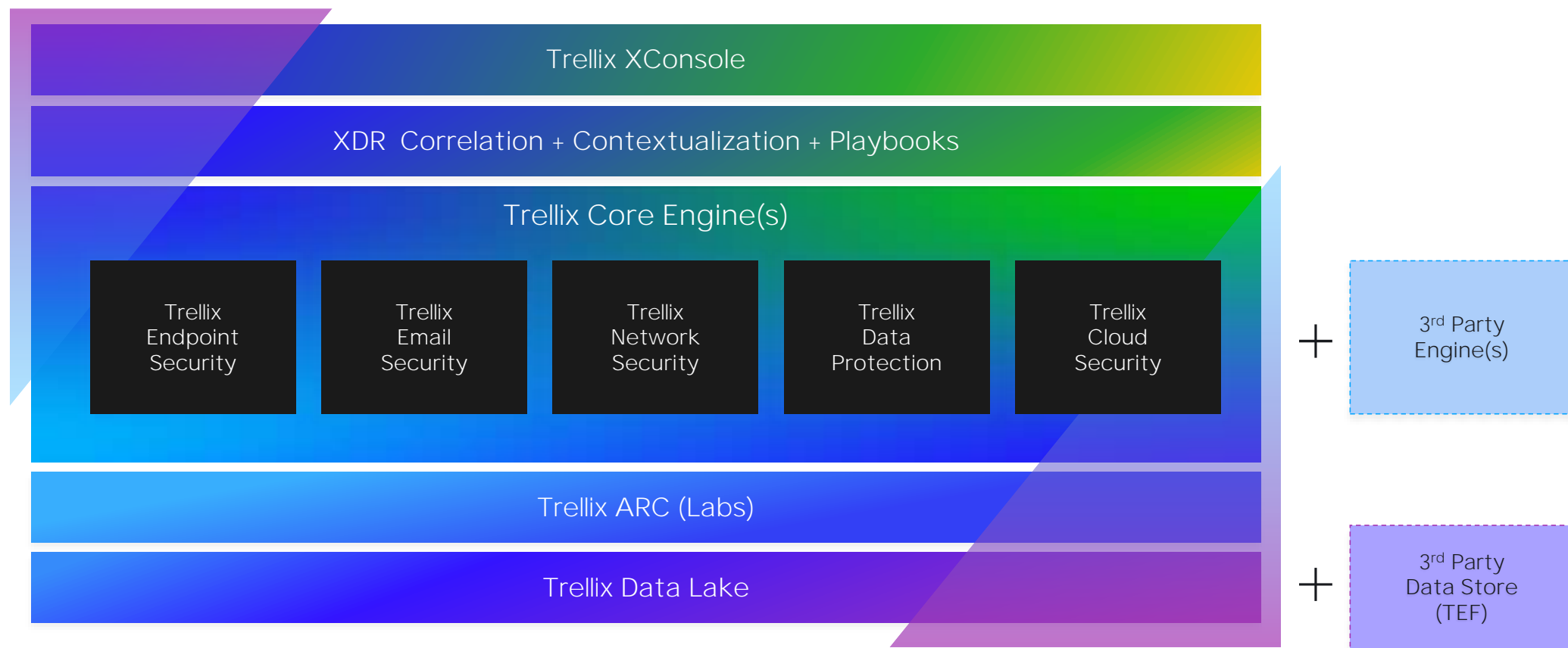
75<sub>days</sub>

Average time it takes to  
discover a breach

30<sub>days</sub>

Average time it takes to  
respond to a breach

# Trellix XDR Platform



# Trellix Platform Overview



## Technology



Flexible Integrations



Data Lake



Detection Analytics



Cloud Visibility

## Processes



Threat Response Enrichment



Guided Investigation



Compliance Reporting

## Expertise



Tailored Content

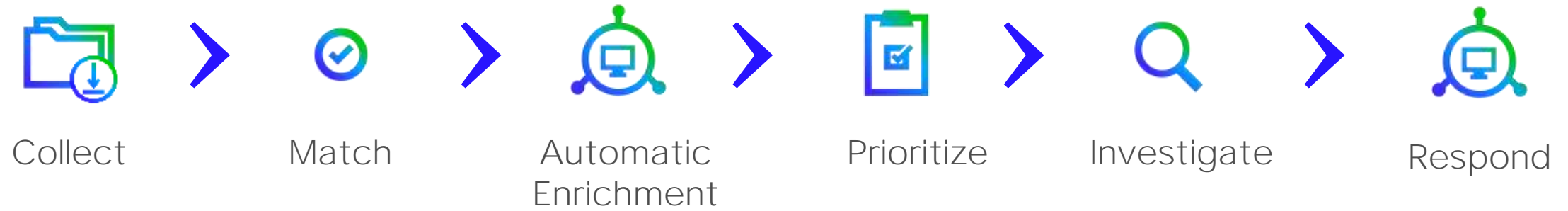


Threat Intelligence



Risk Prioritization

# Trellix Platform in Action














# Welcome to your Dashboard, Tom

There are **367** threats. **240** of them must be reviewed as soon as possible and **127** recommended to be reviewed proactively.

Show: Past 7 Days

Top 6 Threats
View All 40 Threats

Threats: All
Status: Open
Assignee: All
Tags: All
Show: Past 7 Days

<div>  629 </div> <div> CORRELATIONS   ID: 2872   DETECTED AT: 2021-10-12T02:59:03.671311Z BY FIREEYE </div> <div> Did not block Collection(+8) by using Clipboard Data(+22) against system(+2) with malware.binary.doc(+3) </div> <div> <div>Open</div> <div>Unassigned</div> <div>  </div> </div> <div> <div>ENRICHMENT</div> </div>			
<div>  596 </div> <div> CORRELATIONS   ID: 2488   DETECTED AT: 2021-10-08T04:41:13... </div> <div> Did not block Credential Access(+4) by using Command and Scri... </div> <div> <div>Open</div> <div>Unassigned</div> <div>  </div> </div> <div> <div>MULTIPLE (2)</div> </div>			
<div>  500 </div> <div> CORRELATIONS   ID: 2849   DETECTED AT: 2021-10-11T19:30:14... </div> <div> Multiple matches test campaign </div> <div> <div>Open</div> <div>System User</div> <div>  </div> </div> <div> <div>VIP</div> </div>			
<div>  380 </div> <div> CORRELATIONS   ID: 2496   DETECTED AT: 2021-10-08T10:23:16... </div> <div> Did not block Command and Control(+2) by using Drive-by Com... </div> <div> <div>Open</div> <div>Unassigned</div> <div> </div> </div>			
<div>  368 </div> <div> CORRELATIONS   ID: 2365   DETECTED AT: 2021-10-07T07:21:02... </div> <div> Did not block Threat using test.eicar.1(+16) </div> <div> <div>Open</div> <div>Unassigned</div> <div> </div> </div>			
<div>  240 </div> <div> CORRELATIONS   ID: 2242   DETECTED AT: 2021-10-06T07:18:01... </div> <div> Did not block Threat using pdftriggeraction(+11) </div> <div> <div>Open</div> <div>Unassigned</div> <div> </div> </div>			



Assigned Threats
Threats: All Threats
Show: Past 7 Days

System...	
JR	

Threat Intel Matches

← BACK TO THREATS

ID: 2872



Correlations Details

Export

Actions

About



Did not block Collection(+8) by using Clipboard Data(+22) against system(+2) with malware.binary.doc(+3)

ENRICHMENT

9/14 TACTICS



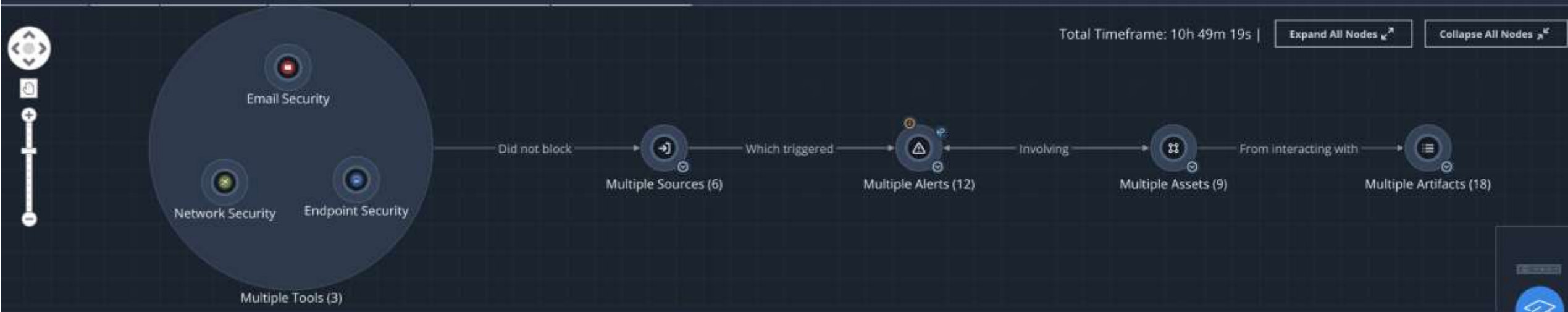
Open

Unassigned

Email Security and Endpoint Security Did not block Collection, Command and Control, Credential Access, Defense Evasion, Discovery, Execution, Initial Access, Privilege Escalation, Resource Development by using Clipboard Data, Command and Scripting Interpreter, DCSync, DNS, File Deletion, Hidden Files and Directories, LSA Secrets, LSASS Memory, Malicious File, Malware, Malware, Native API, OS Credential Dumping, Phishing, PowerShell, PowerShell, Process Injection, Query Registry, Security Account Manager, Spearphishing Attachment, Template Injection, Visual Basic, Windows Management Instrumentation against system, victim-7fhs0h5, VICTIM-7FHS0H5 with malware.binary.doc, password\_extraction\_success, binary.doc, fec\_dropper\_poxml\_generic\_1.

Last Seen: 2021-10-12 | 03:00:31 UTC (11 hours ago)

Overview Intel Events 54 Related Alerts 12 Related Assets 3 Orchestration 24





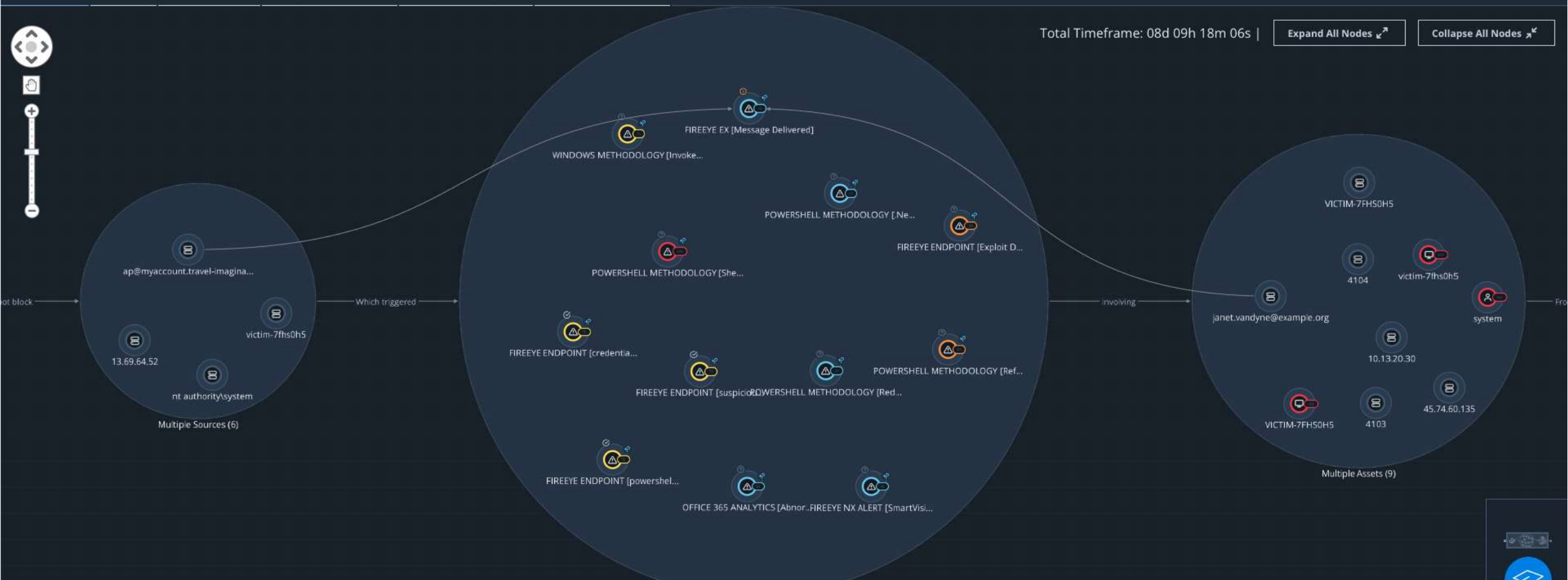
[← BACK TO THREATS](#)
 ID: 2872
 
 Correlations Details

[Export](#)
[Actions](#)

629
 Did not block Collection(+9) by using Clipboard Data(+23) against system(+2) with fec\_dropper\_ooxml\_generic\_1(+3)
 [MULTIPLE \(3\)](#)
[10/14 TACTICS](#)

 --- Open
 Elazar

[Overview](#)
[Intel](#)
[Events 61](#)
[Related Alerts 12](#)
[Related Assets 3](#)
[Orchestration 72](#)



# Proof Points

Visibility

650+

Product integrations to minimize pivot points and accelerate response

Response Time

20x

Acceleration in manual tasks like alert enrichment and triage

Value

5-7

Stand-alone product capabilities combined in one platform

Efficiency

86%

Reduction in analyst time spent on non-response activities



# 600+ Integrations and Counting



Trellix



Halle 7  
Stand 420

bei unserem Partner



**INFINIGATE**

.... Adding Value to Distribution

