Introduction to Elastic Security:
Modernizing Security Operations

Alessandro Brofferio, Elastic

March 16th, 2022

We build search solutions on a single platform

- Enterprise Search
- Observability
- **Security**

elastic

The Elastic Search Platform

elastic

Data is at the heart of modern enterprise.

Data is at the heart of modern security.

Global trends driving rapid change

Security challenges are compounding quickly

Trend #1:

Digital transformation

175ZB

predicted worldwide data growth by 2025*

288

# of apps the average enterprise must manage**

Trend #2:

Motivated adversaries

$1.1T

2020 global cost of cybercrime, growing 35% annually

* IDC, Data Age 2025 report
** Blissfully, 2020 Annual SaaS Trends report
*** Cybersecurity Ventures, Cyberwarfare in the C-Suite report, 2020
**** Infosecurity Magazine, Evasive Malware Threats on the Rise article

elastic

What outcomes do we care about?

speed, scale, relevance

Shorter dwell times, minimal damage

Faster remediation of complex threats

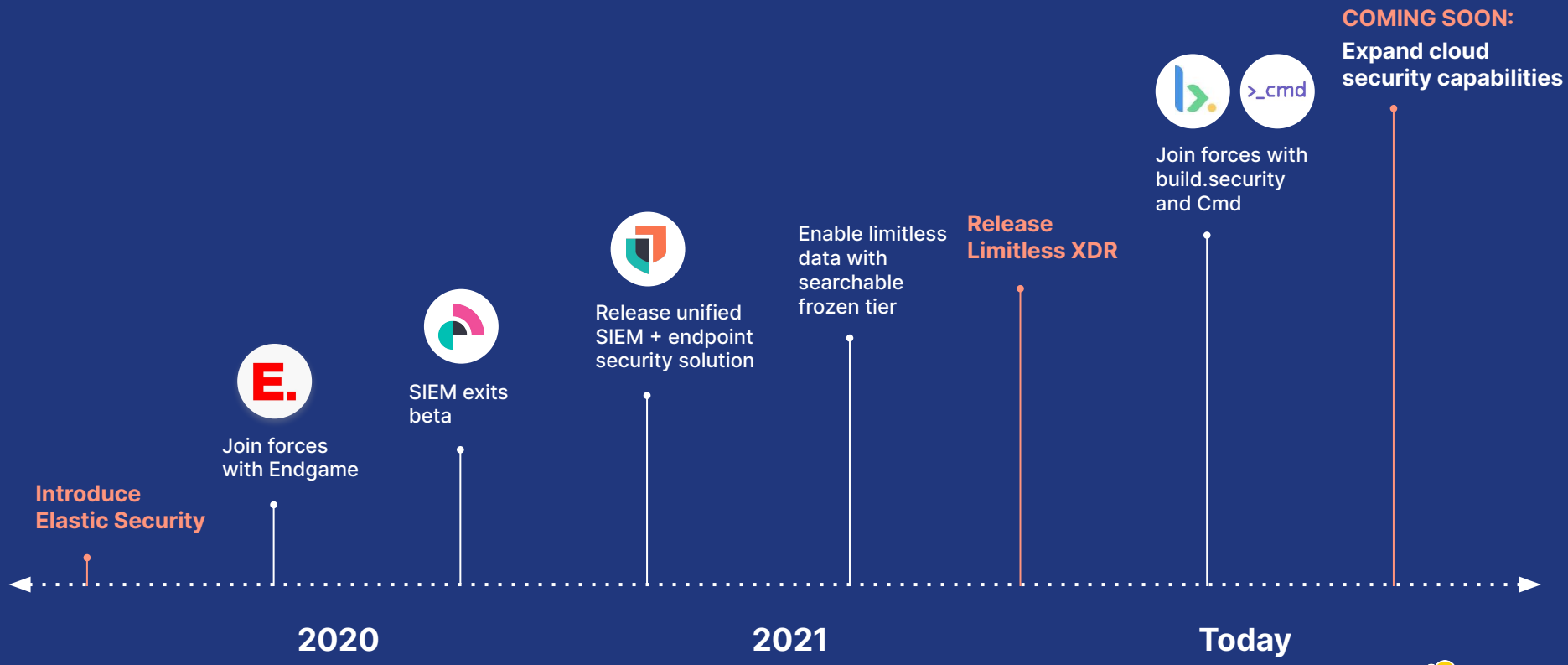
Accelerated investigation and response

elastic

The Evolution of Elastic Security

elastic

Elastic Security



elastic

Limitless

Visibility
Data
Analysis
Prevention & Detection
Value

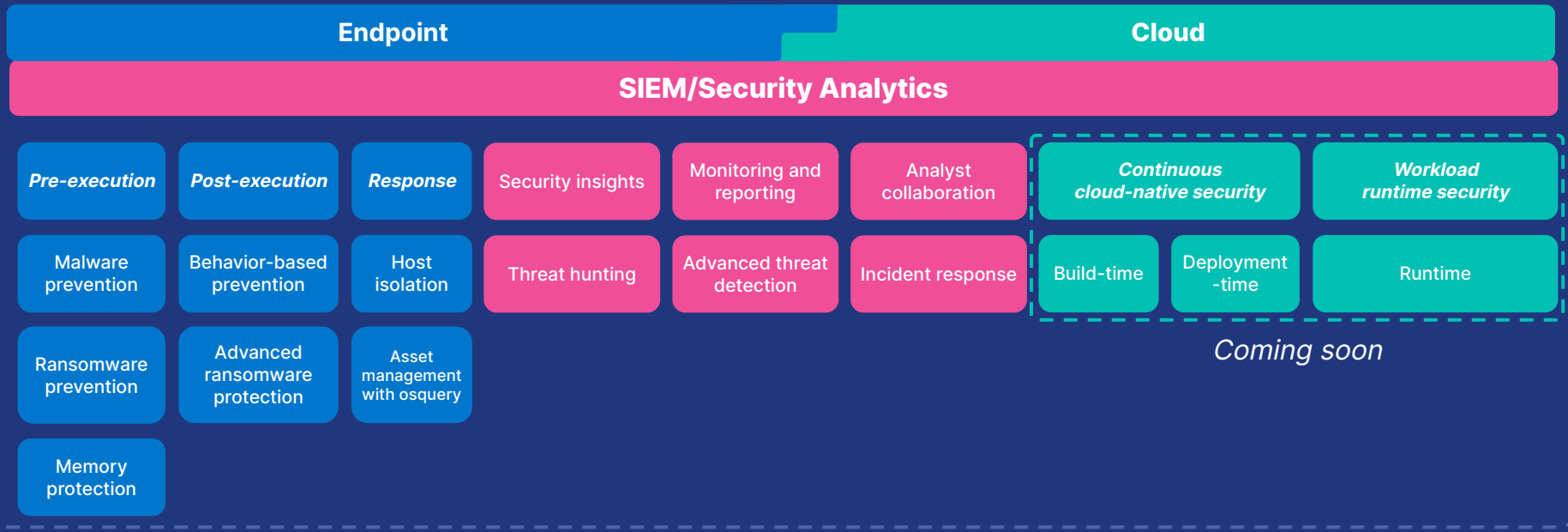
XDR

XDR modernizes security operations, enabling analytics across all data, automating key processes, and bringing native endpoint security to every host.

elastic

Elastic Security

Security without Limits



Elastic Security

Limitless XDR

SIEM

Endpoint Security

Cloud Security

elastic

Elastic Security

Prevent

Pre-execution prevention
- ❑ Malware prevention
- ❑ Ransomware prevention

Post-execution prevention
- ❑ Behavioral ransomware Prevention

Collect

Continuous visibility
- ❑ Kernel-level data collection
- ❑ Tailored host data collection
- ❑ Ad-hoc host analysis via osquery

Elastic Agent

Detect

- ❑ Alert triage and hunting workflows
- ❑ Insights, context, and recommendations
- ❑ Threat intel. integrations
- ❑ Prebuilt detections: use cases, rules, ML models
- ❑ Advanced analytics, interactive visualizations, root-cause analysis
- ❑ Fast and scalable search platform, open data schema, on-prem to multi-cloud

Elastic Stack

Respond

- ❑ Investigation & response workflows
- ❑ External alert actions: email, Slack, SOAR & ITSM platforms
- ❑ External case connectors: IBM, JIRA, ServiceNow, Swimlane
- ❑ Simple custom connections

Elastic Stack

- ❑ On-demand osquery inspection
- ❑ Remote host isolation

Elastic Agent

Before Searchable Snapshots

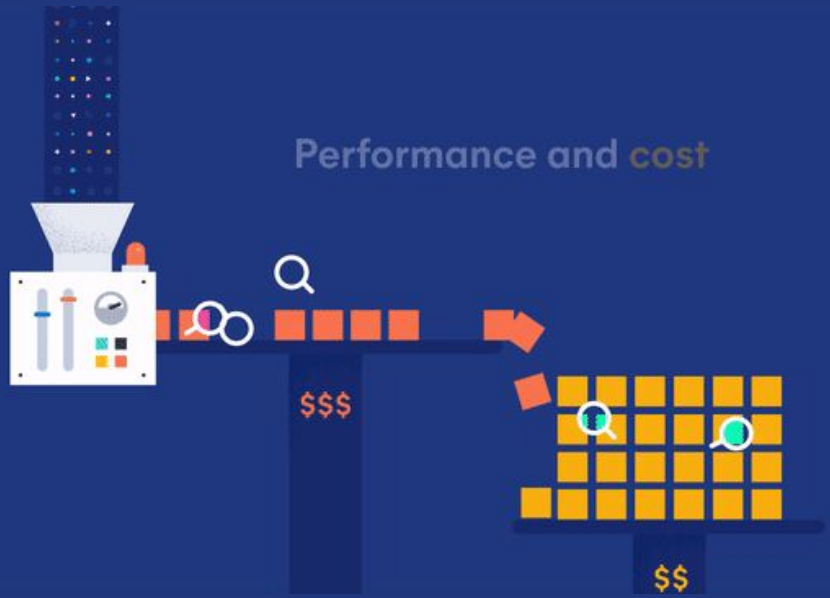
During Incident Response:

- Realize that you need historical archived data
- Find out where it's stored
- Arranged for the volume to be mounted/bucket to be made available
- Ensure cluster and licensing capacity exists for restore
- Wait for restore to complete
- Search

With Searchable Snapshots

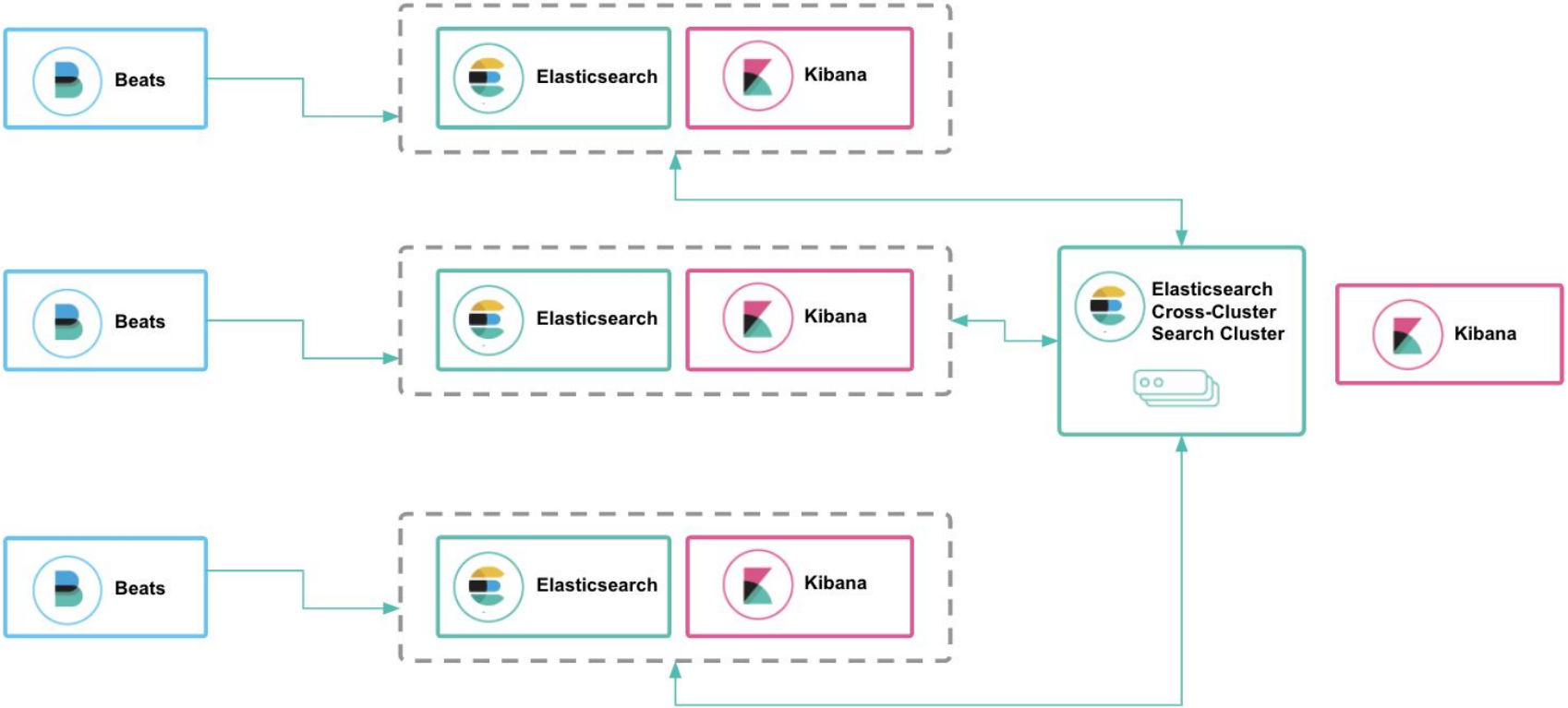
During Incident Response:

- Search!

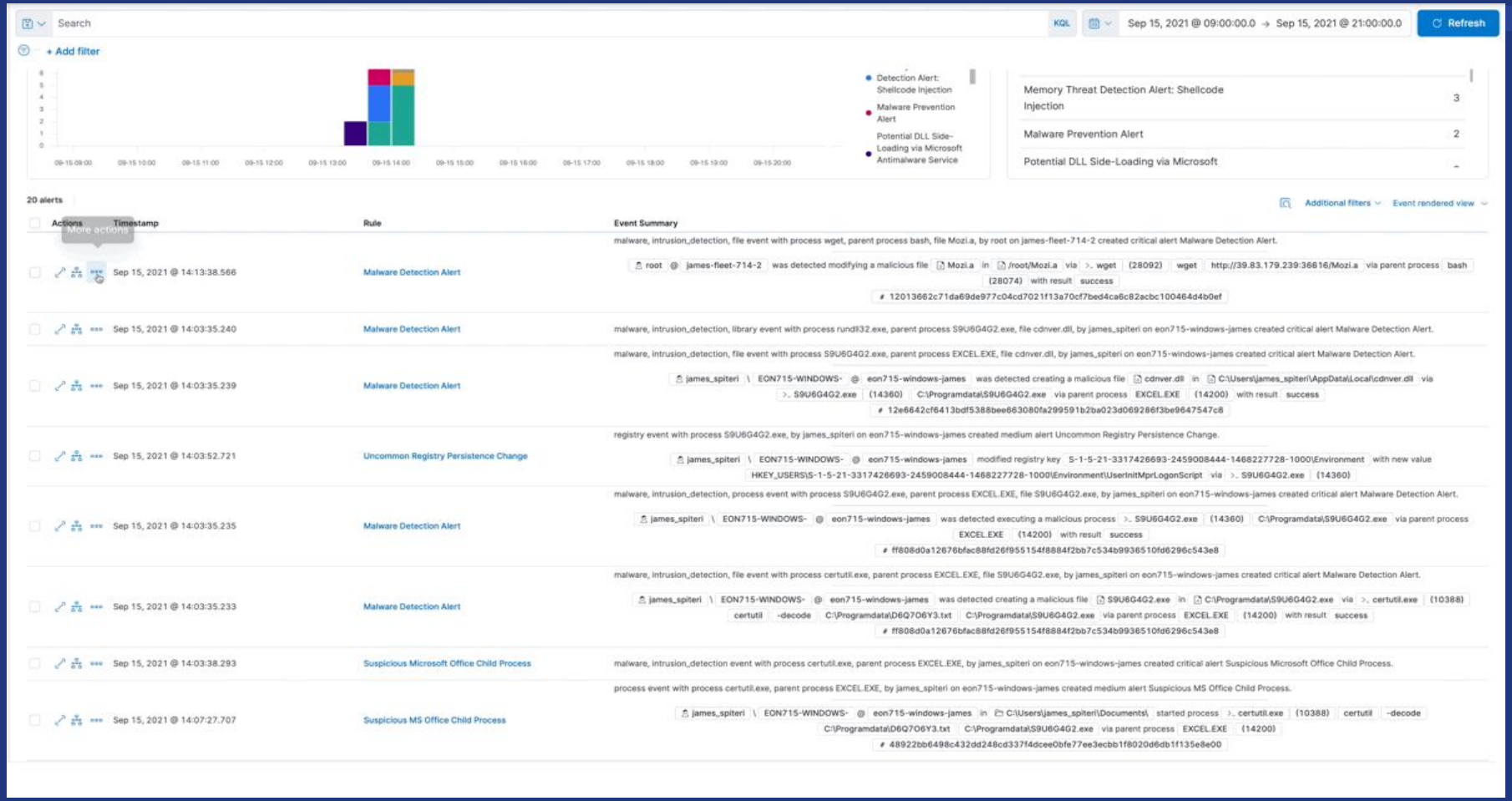


elastic

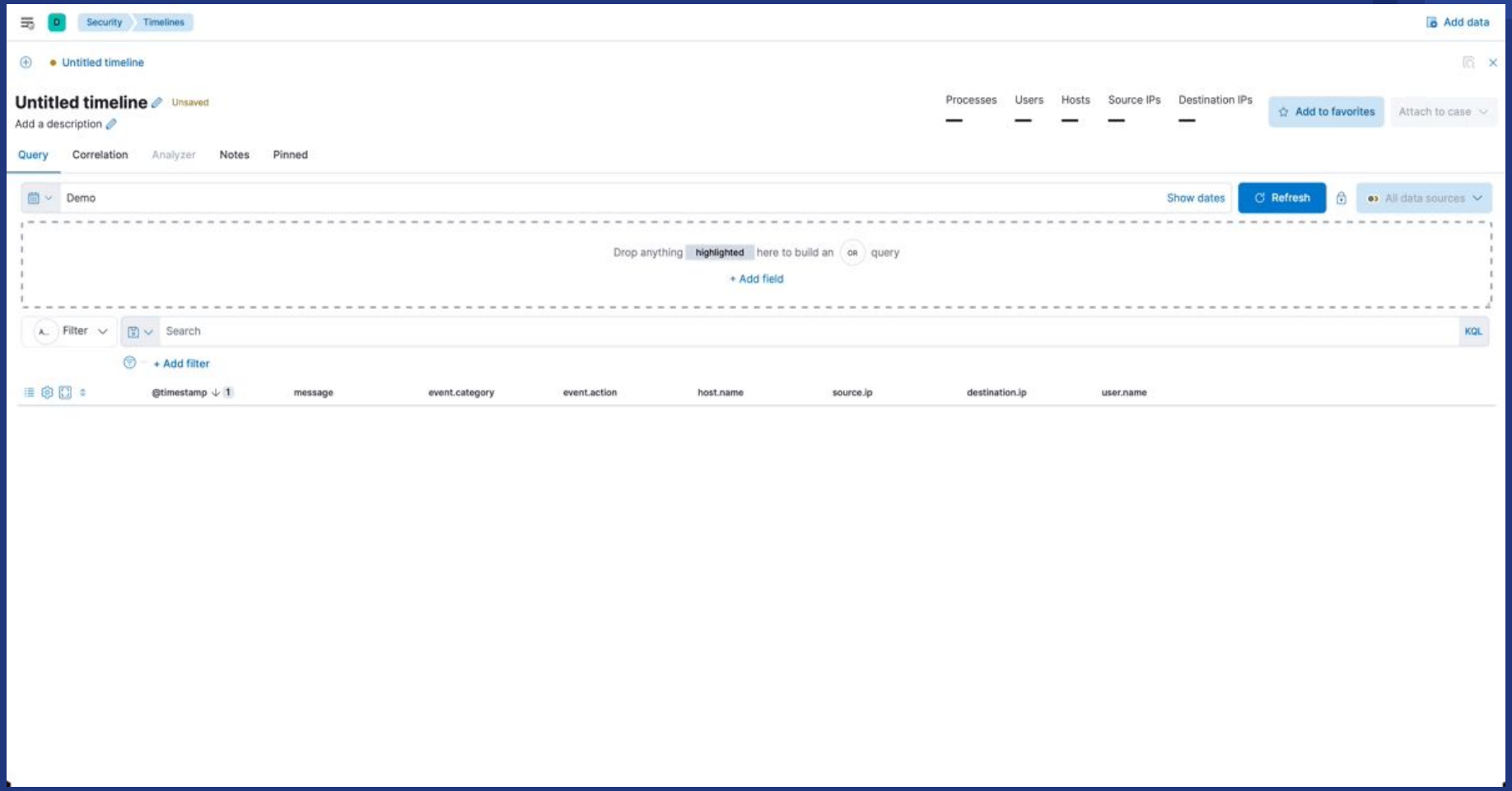
Cross-Cluster Search



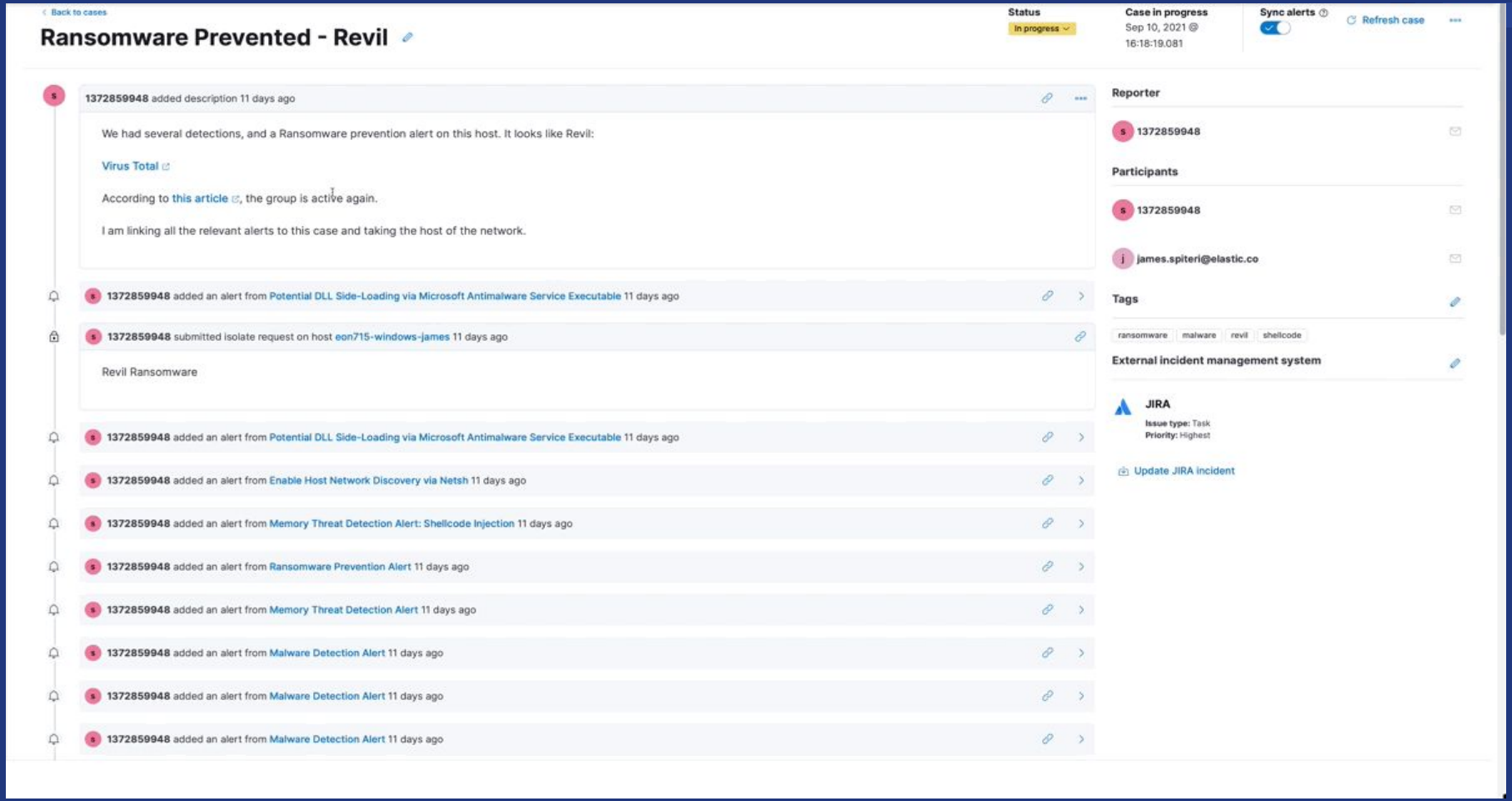
Event Analyzer



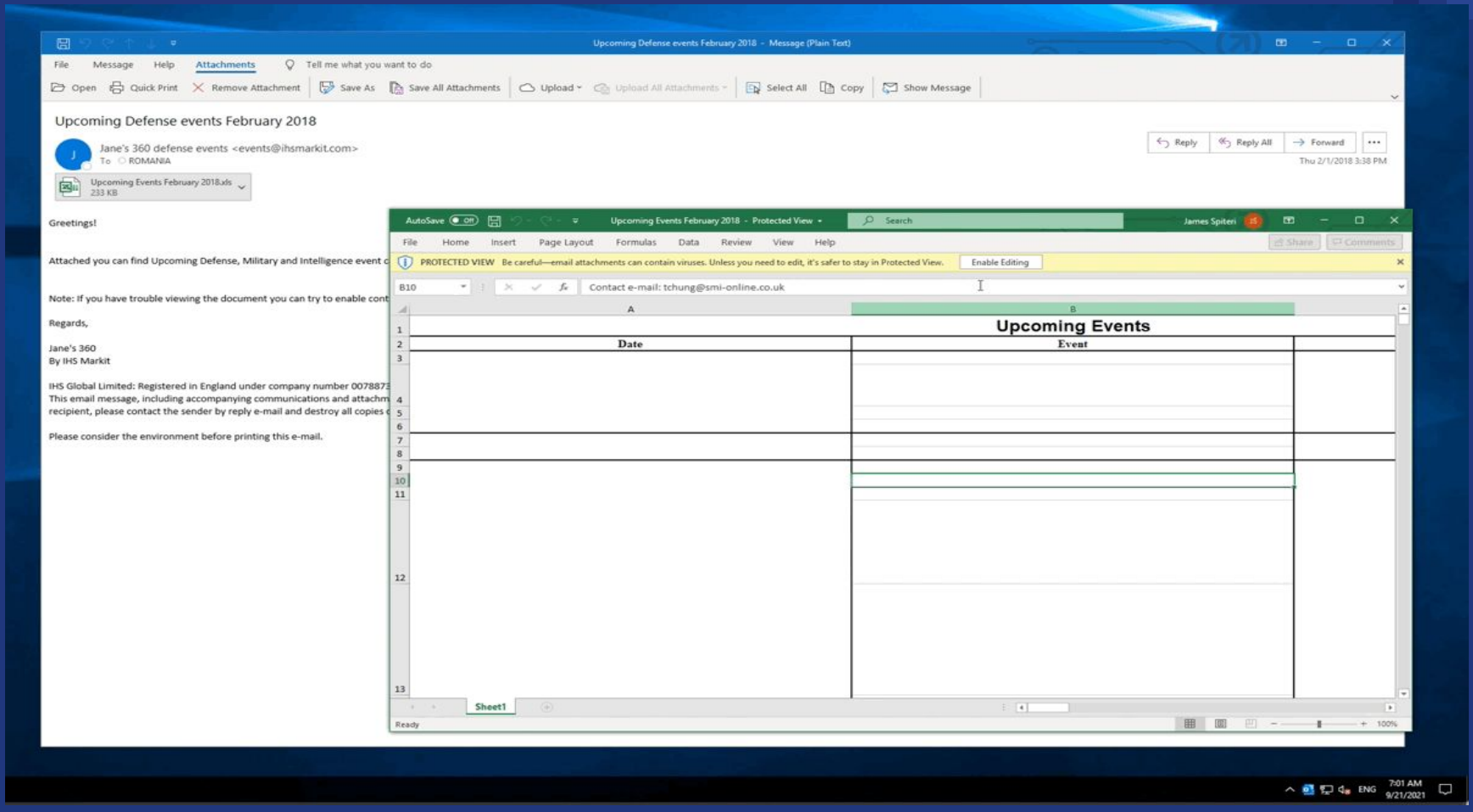
Correlation in Timeline



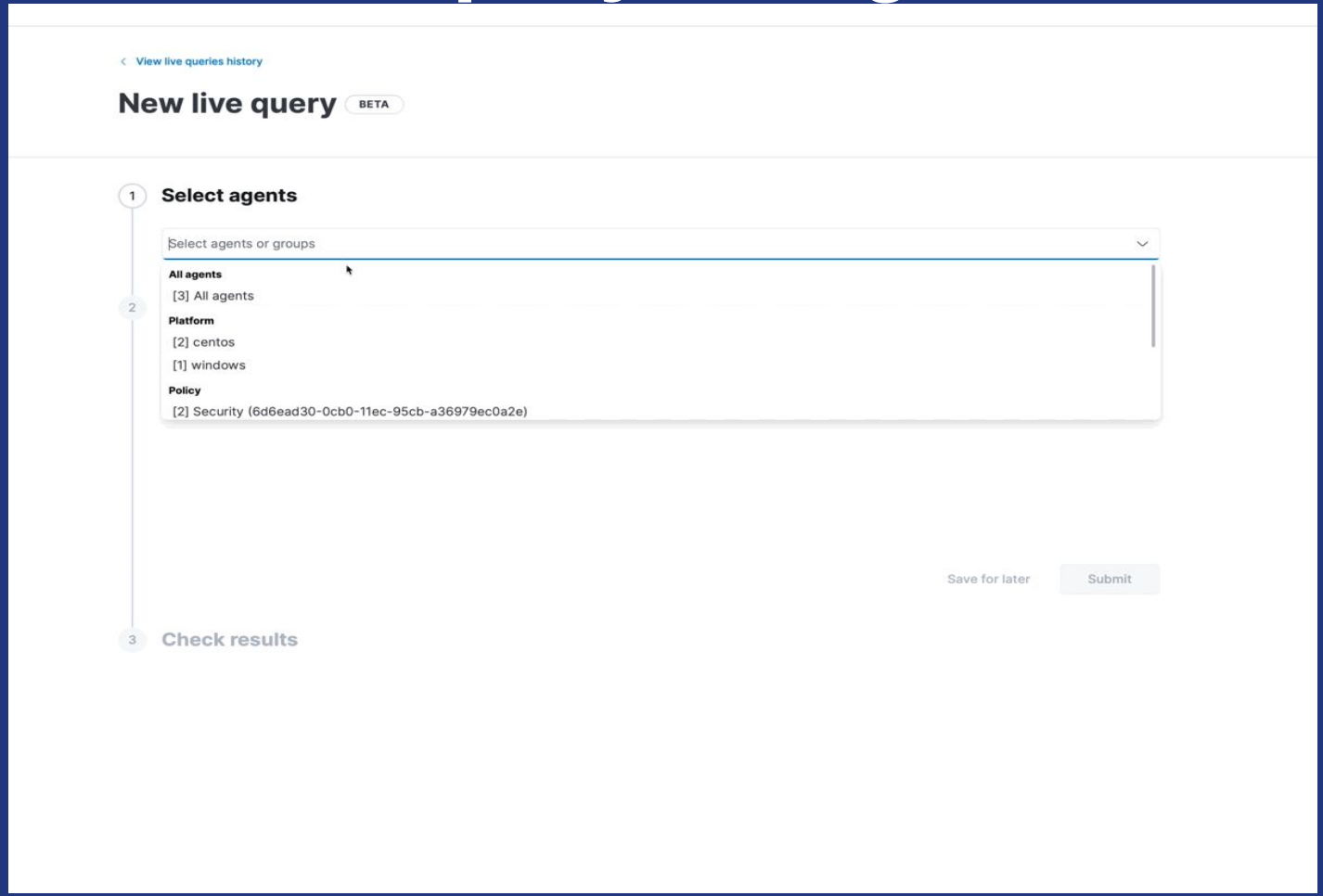
Case Management



Endpoint Response Actions



Osquery Management



Elastic for Students and Educators Program Vision

https://www.elastic.co/community/students-and-educators
https://www.elastic.co/fr/community/students-and-educators/faq

Elastic Cloud

Give them the tools they need to be successful

Provide students and educators with free access to our products to use for personal projects, research and/or curriculum design.

Training and Resource Access

Give them the tools and teach them how to use them.

Provide access to a resource library comprised of on-demand courses and trainings, virtual workshops/demos and product guides to help students and educators explore our products and develop a solid foundation and diverse skill set.

Community Engagement

Bring them into the Elastic community.

Create pathways for students and educators to connect and engage with the Elastic community. Connecting students and educators with industry leaders and customers.

Get started with Elastic Security

Learn more:
ela.st/modern-siem

Try for free:
ela.st/siem

Engage with us:
ela.st/slack

elastic

Thank you

elastic.co/security