



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



The Elastic Search Platform



**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](#)

What outcomes do we care about?

speed, scale, relevance



Shorter dwell times,
minimal damage



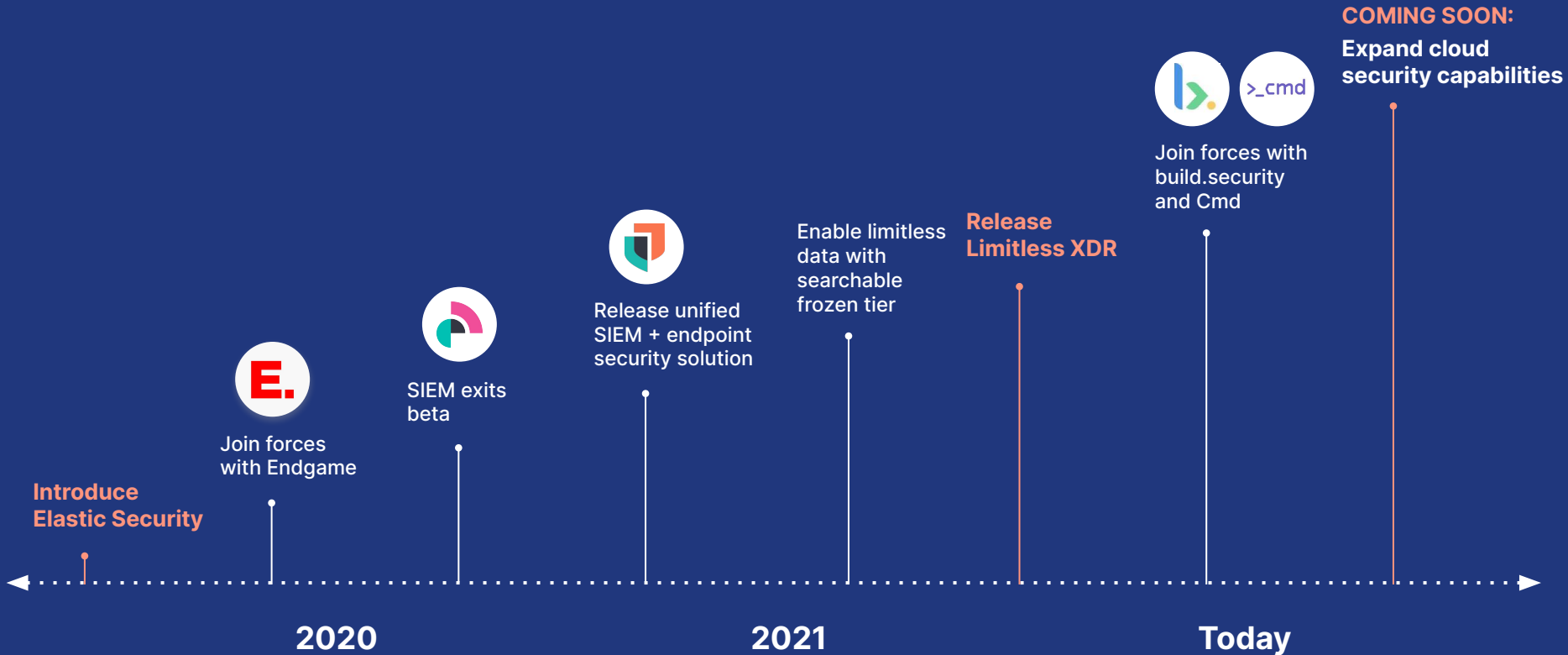
Faster remediation
of complex threats



Accelerated
investigation and
response

The Evolution of Elastic Security

Elastic Security





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.

Security without Limits

Endpoint

Cloud

SIEM/Security Analytics

Pre-execution

Post-execution

Response

Security insights

Monitoring and reporting

Analyst collaboration

Continuous cloud-native security

Workload runtime security

Malware prevention

Behavior-based prevention

Host isolation

Threat hunting

Advanced threat detection

Incident response

Build-time

Deployment-time

Runtime

Ransomware prevention

Advanced ransomware protection

Asset management with osquery

Memory protection

Coming soon

Limitless XDR

SIEM

**Endpoint
Security**

**Cloud
Security**



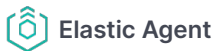
Prevent

- 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



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



Respond

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



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



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

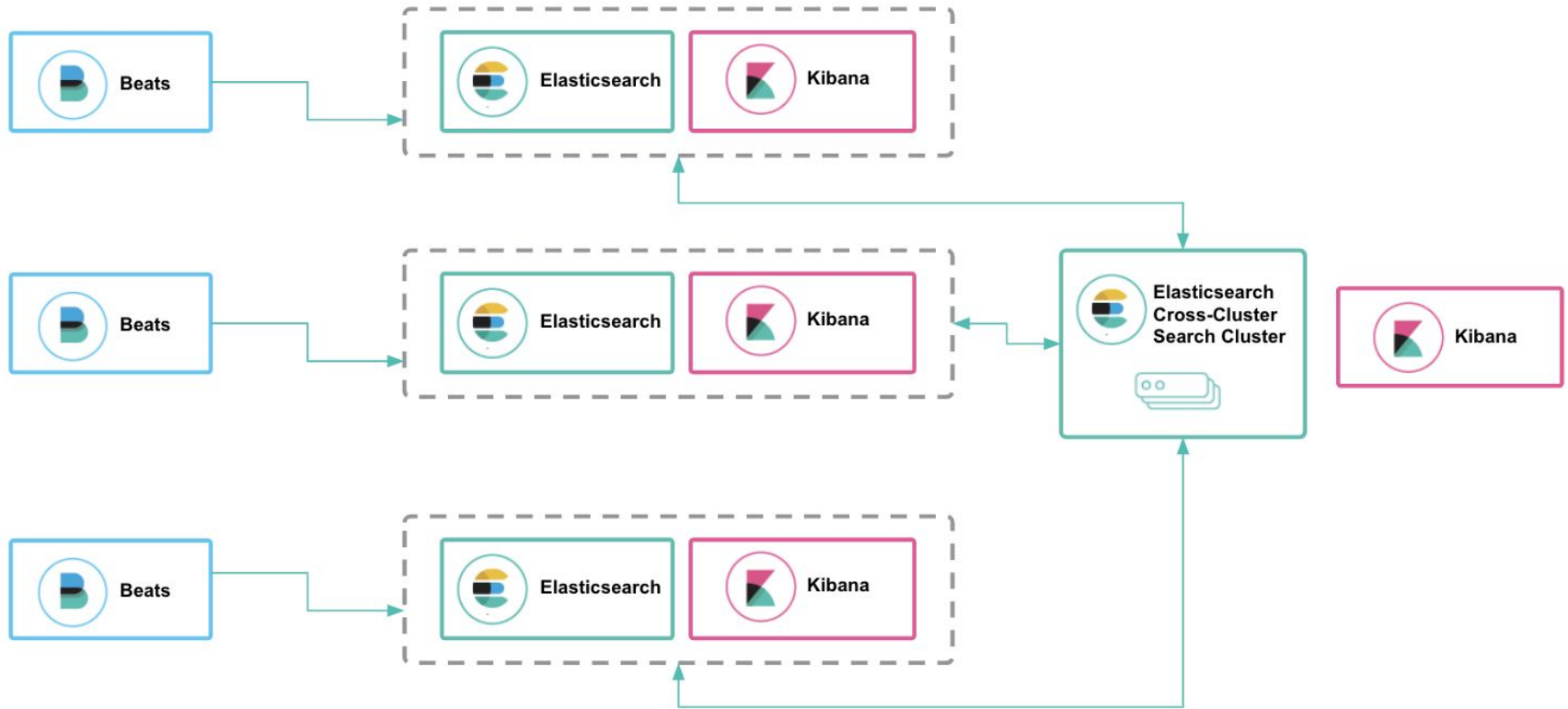
With Searchable Snapshots

During Incident Response:

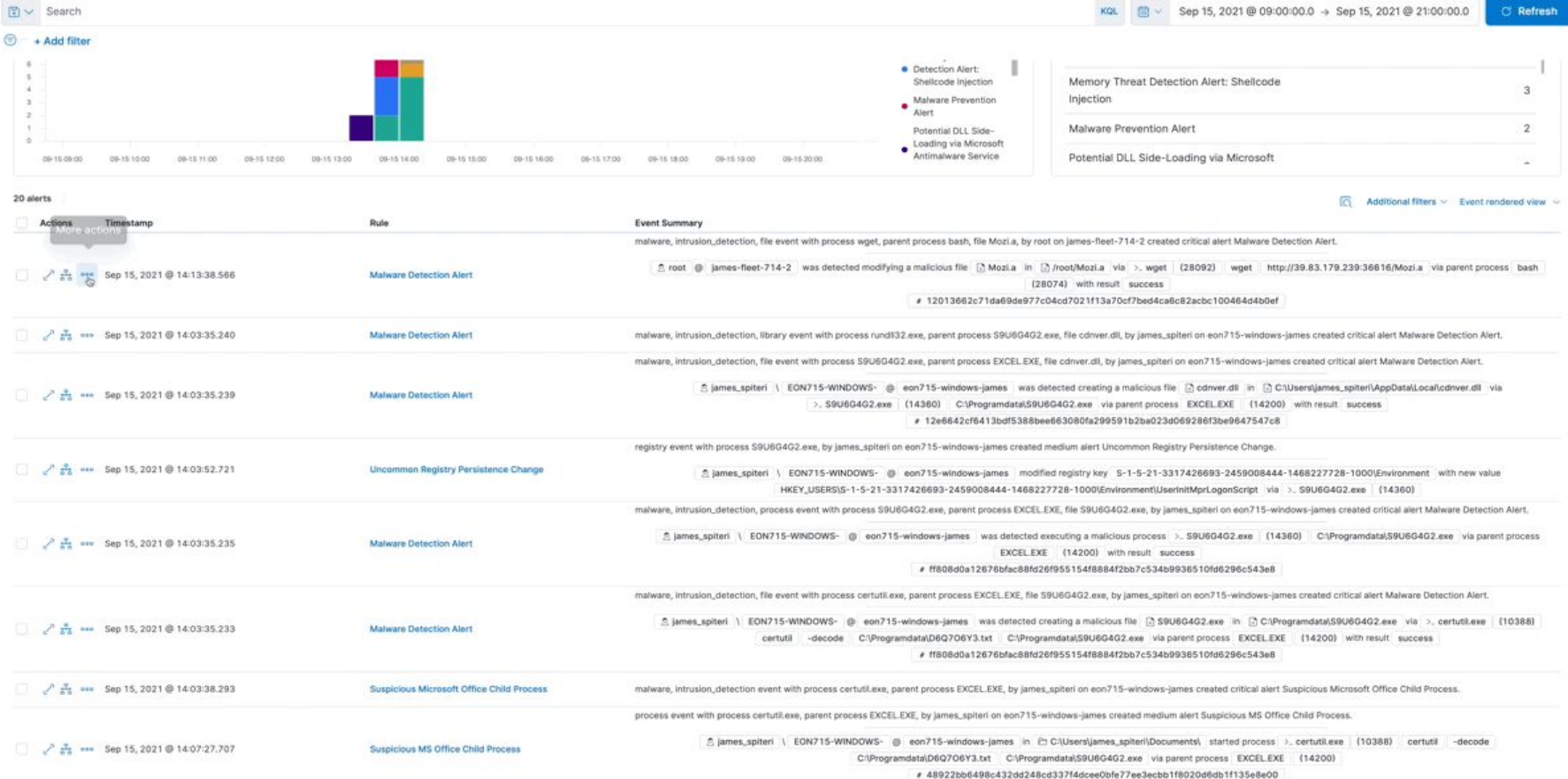
- Search!



Cross-Cluster Search



Event Analyzer



Correlation in Timeline

The screenshot displays a security timeline interface. At the top, there are navigation tabs for 'Security' and 'Timelines', and an 'Add data' button. Below this, the current timeline is named 'Untitled timeline' and is marked as 'Unsaved'. A description field is available. The main interface is divided into several sections:

- Navigation:** 'Query', 'Correlation', 'Analyzer', 'Notes', and 'Pinned' tabs are visible, with 'Correlation' currently selected.
- Timeline Header:** Includes a 'Demo' dropdown, 'Show dates', a 'Refresh' button, a lock icon, and an 'All data sources' dropdown.
- Query Builder:** A large dashed box contains the instruction 'Drop anything highlighted here to build an OR query' and an '+ Add field' button.
- Filter and Search:** A 'Filter' dropdown and a 'Search' input field are present, along with an '+ Add filter' button.
- Field List:** A row of fields is shown: '@timestamp', 'message', 'event.category', 'event.action', 'host.name', 'source.ip', 'destination.ip', and 'user.name'. The '@timestamp' field is currently selected.

Case Management

[Back to cases](#)

Ransomware Prevented - Revil

Status

In progress

Case in progress

Sep 10, 2021 @

16:18:19.081

Sync alerts



[Refresh case](#)



5

1372859948 added description 11 days ago

We had several detections, and a Ransomware prevention alert on this host. It looks like Revil:

[Virus Total](#)

According to [this article](#), the group is active again.

I am linking all the relevant alerts to this case and taking the host of the network.



1372859948 added an alert from [Potential DLL Side-Loading via Microsoft Antimalware Service Executable](#) 11 days ago



1372859948 submitted isolate request on host [eon715-windows-james](#) 11 days ago

Revil Ransomware



1372859948 added an alert from [Potential DLL Side-Loading via Microsoft Antimalware Service Executable](#) 11 days ago



1372859948 added an alert from [Enable Host Network Discovery via Netsh](#) 11 days ago



1372859948 added an alert from [Memory Threat Detection Alert: Shellcode Injection](#) 11 days ago



1372859948 added an alert from [Ransomware Prevention Alert](#) 11 days ago



1372859948 added an alert from [Memory Threat Detection Alert](#) 11 days ago



1372859948 added an alert from [Malware Detection Alert](#) 11 days ago



1372859948 added an alert from [Malware Detection Alert](#) 11 days ago



1372859948 added an alert from [Malware Detection Alert](#) 11 days ago

Reporter

1372859948

Participants

1372859948

[james.spiteri@elastic.co](#)

Tags

[ransomware](#) [malware](#) [revil](#) [shellcode](#)

External incident management system

JIRA

Issue type: Task

Priority: Highest

[Update JIRA incident](#)

Endpoint Response Actions

Upcoming Defense events February 2018 - Message (Plain Text)

File Message Help **Attachments** Tell me what you want to do
 Open Quick Print Remove Attachment Save As Save All Attachments Upload Upload All Attachments Select All Copy Show Message

Upcoming Defense events February 2018

Jane's 360 defense events <events@ihsmarkit.com>
 To: ROMANIA

Upcoming Events February 2018.xls
 233 KB

Greetings!

Attached you can find Upcoming Defense, Military and Intelligence event calendar for February 2018.

Note: If you have trouble viewing the document you can try to enable content. Right-click on the attachment and select "Open Content Advisor Settings" and then click "Yes, I want to enable content."

Regards,
 Jane's 360
 By IHS Markit

IHS Global Limited: Registered in England under company number 0078872
 This email message, including accompanying communications and attachments, is confidential and intended solely for the individual named. If you are not the named recipient, please contact the sender by reply e-mail and destroy all copies of this message. Do not disseminate, distribute, or take any action in reliance on the information contained herein.

Please consider the environment before printing this e-mail.

Upcoming Events February 2018 - Protected View

File Home Insert Page Layout Formulas Data Review View Help

PROTECTED VIEW Be careful—email attachments can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

B10 Contact e-mail: tchung@smi-online.co.uk

A		B	
Date		Upcoming Events	
Event			

Sheet1

Ready 100%

Osquery Management

[View live queries history](#)

New live query BETA

1 Select agents

Select agents or groups

All agents

[3] All agents

Platform

[2] centos

[1] windows

Policy

[2] Security (6d6ead30-0cb0-11ec-95cb-a36979ec0a2e)

Save for later

Submit

3 Check results



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



Thank you

elastic.co/security