elastic | The Search Analytics Company

v

Switch to Elastic Security

Modernize SecOps

Stefano Radaelli - Solution Architect

Modernize security operations with the power of data

Eliminate blind spots and reduce OpEx

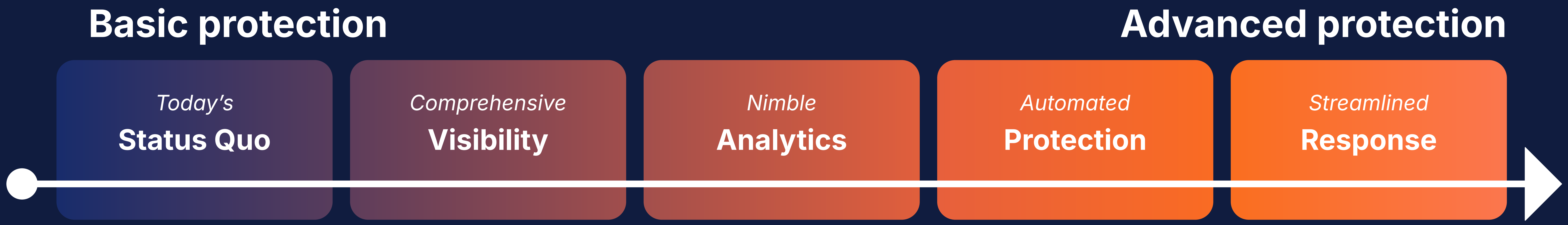
Swiftly search years of archives

Protect everywhere with ML jobs and rules

Arm analysts with AI insights and guidance

Harness hybrid and multi-cloud support

Security teams need a unified solution



Basic protection

Advanced protection

Today's **Status Quo**

- Data blind spots and silos
- Inconsistent data formatting

Comprehensive **Visibility**

- Single data store
- Data preparation
- Extended lookback

Nimble **Analytics**

- Querying and pivoting
- Cloud scale

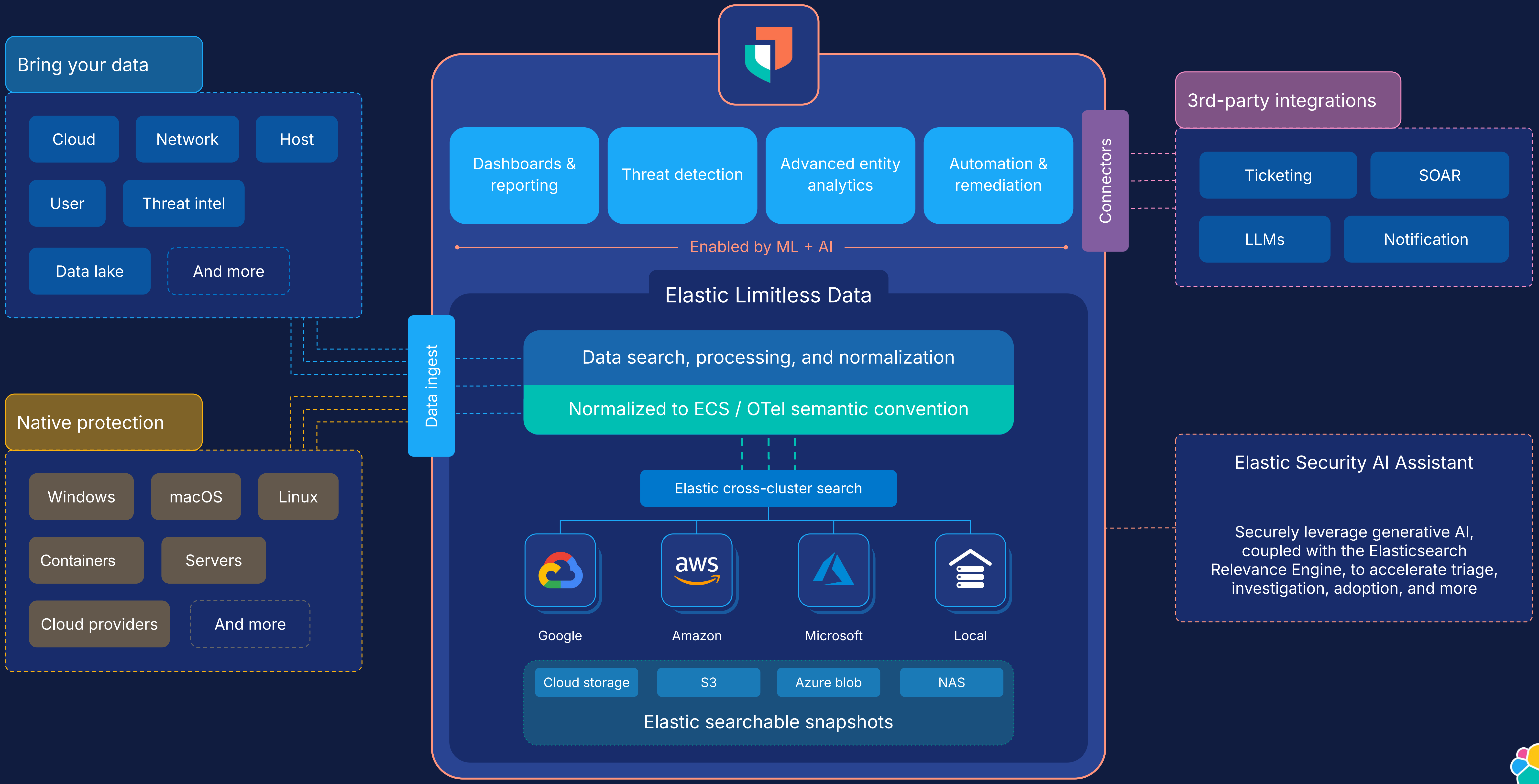
Automated **Protection**

- Prebuilt protections aligned with MITRE ATT&CK
- Turnkey ransomware and malware prevention
- Centralized detection
- Cloud workload protection
- Threat intel. matching

Streamlined **Response**

- Standardized workflows
- Informed investigations
- Automated responses
- Seamless host inspection

Elastic Security



Bring your data

Cloud

Network

Host

User

Threat intel

Data lake

And more

Native protection

Windows

macOS

Linux

Containers

Servers

Cloud providers

And more

Data ingest

Dashboards & reporting

Threat detection

Advanced entity analytics

Automation & remediation

Enabled by ML + AI

Connectors

Elastic Limitless Data

Data search, processing, and normalization

Normalized to ECS / OTel semantic convention

Elastic cross-cluster search

Google

Amazon

Microsoft

Local

Cloud storage

S3

Azure blob

NAS

Elastic searchable snapshots

3rd-party integrations

Ticketing

SOAR

LLMs

Notification

Elastic Security AI Assistant

Securely leverage generative AI, coupled with the Elasticsearch Relevance Engine, to accelerate triage, investigation, adoption, and more

elastic

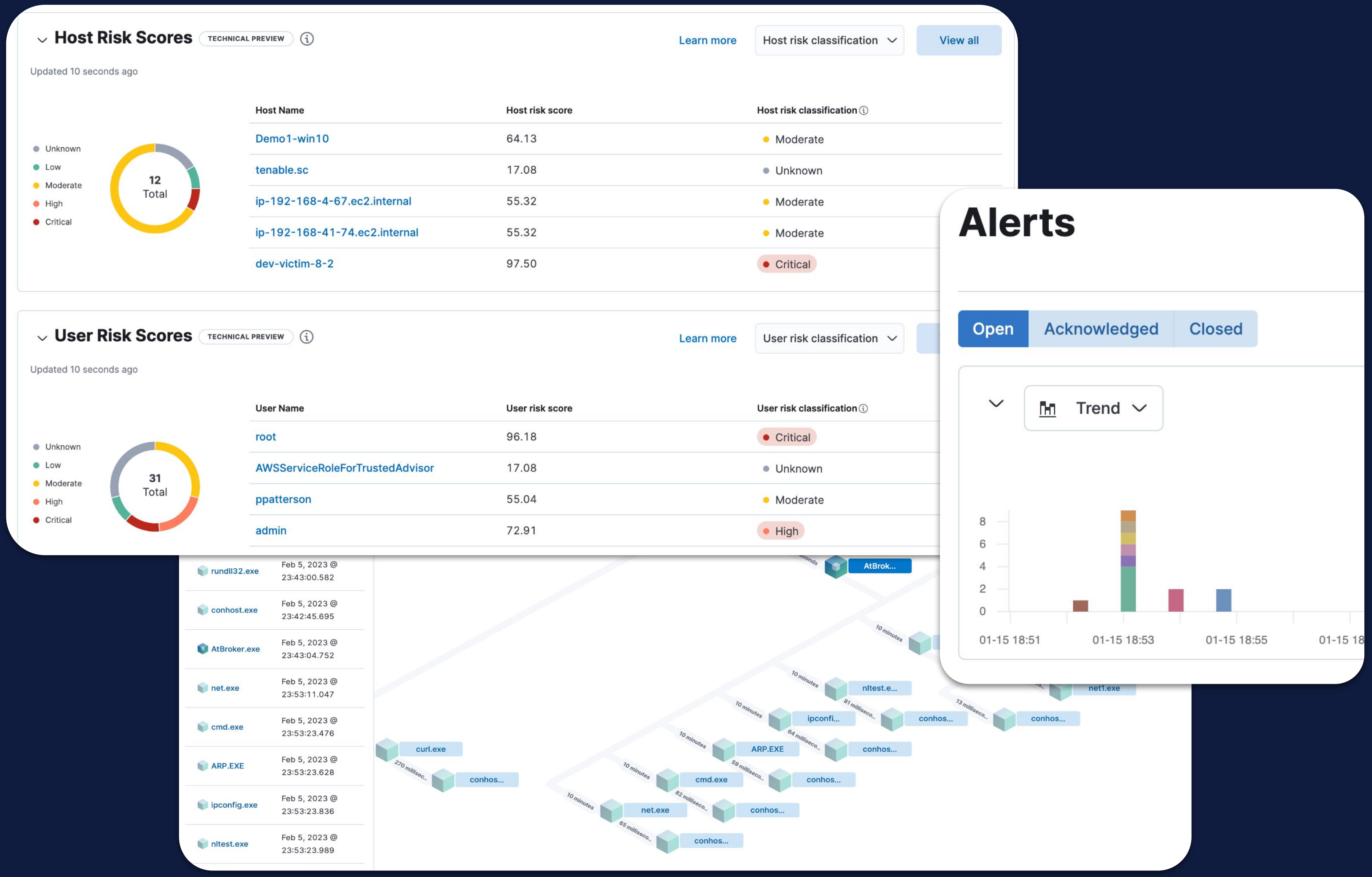
Arm every analyst

Protect → Investigate → Respond

Prevent and detect threats at the outset

Streamline investigation

Remediate the threat in the same workflow



Host Risk Scores

TECHNICAL PREVIEW

Learn more · Host risk classification · View all

Updated 10 seconds ago

● Unknown ● Low ● Moderate ● High ● Critical — 12 Total

Host Name	Host risk score	Host risk classification
Demo1-win10	64.13	● Moderate
tenable.sc	17.08	● Unknown
ip-192-168-4-67.ec2.internal	55.32	● Moderate
ip-192-168-41-74.ec2.internal	55.32	● Moderate
dev-victim-8-2	97.50	● Critical

User Risk Scores

TECHNICAL PREVIEW

Learn more · User risk classification

Updated 10 seconds ago

● Unknown ● Low ● Moderate ● High ● Critical — 31 Total

User Name	User risk score	User risk classification
root	96.18	● Critical
AWSServiceRoleForTrustedAdvisor	17.08	● Unknown
ppatterson	55.04	● Moderate
admin	72.91	● High

rundll32.exe	Feb 5, 2023 @ 23:43:00.582
conhost.exe	Feb 5, 2023 @ 23:42:45.695
AtBroker.exe	Feb 5, 2023 @ 23:43:04.752
net.exe	Feb 5, 2023 @ 23:53:11.047
cmd.exe	Feb 5, 2023 @ 23:53:23.476
ARP.EXE	Feb 5, 2023 @ 23:53:23.628
ipconfig.exe	Feb 5, 2023 @ 23:53:23.836
nltest.exe	Feb 5, 2023 @ 23:53:23.989

Alerts

Open | Acknowledged | Closed

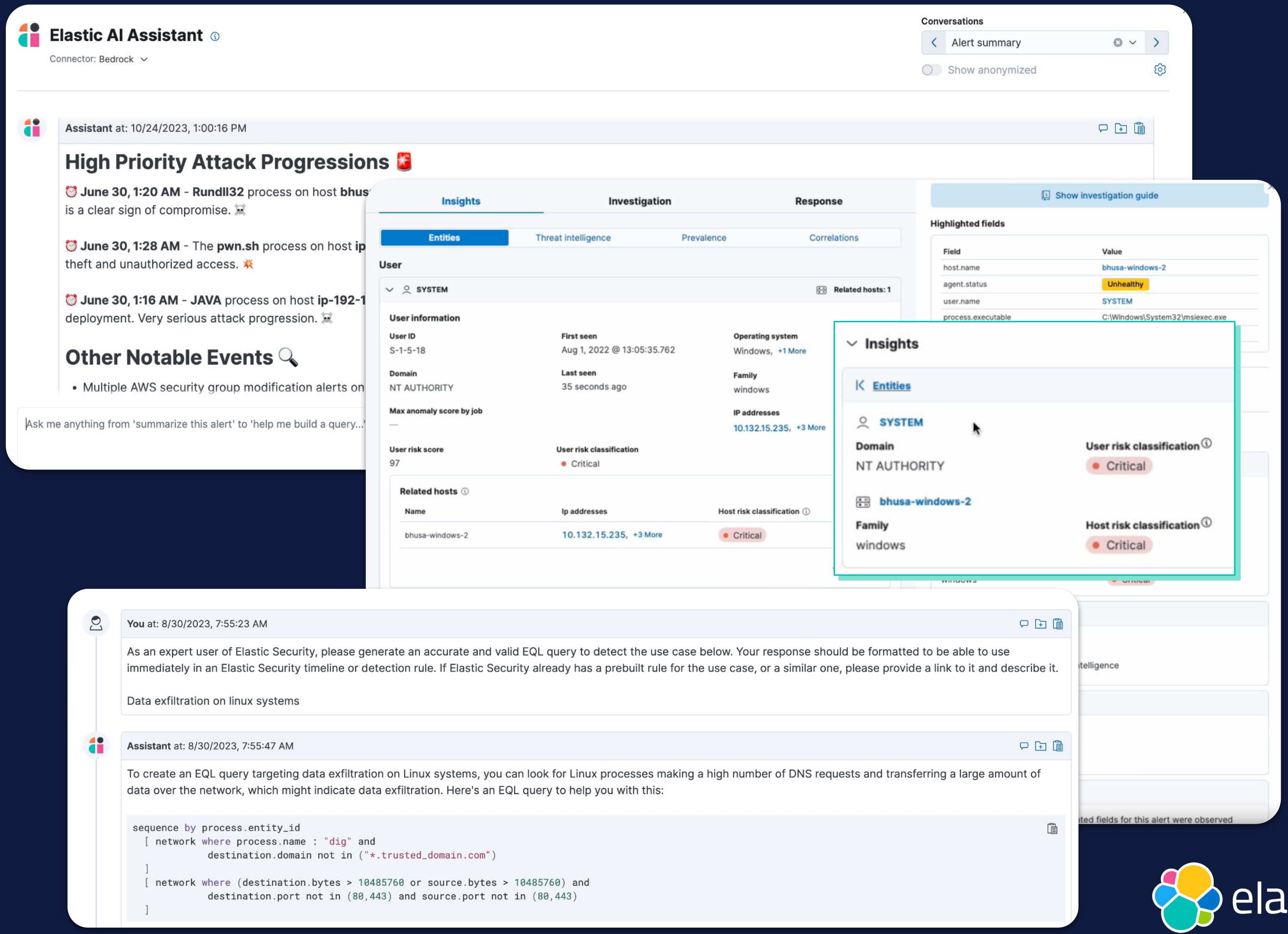
Arm every analyst

Protect → **Investigate** → **Respond**

Prevent and detect threats at the outset

Streamline investigation

Remediate the threat in the same workflow



Assistant at: 10/24/2023, 1:00:16 PM

High Priority Attack Progressions 🚨

⏰ **June 30, 1:20 AM** - **Rundll32** process on host **bhus**
is a clear sign of compromise. ☠

⏰ **June 30, 1:28 AM** - The **pwn.sh** process on host **ip**
theft and unauthorized access. 💥

⏰ **June 30, 1:16 AM** - **JAVA** process on host **ip-192-1**
deployment. Very serious attack progression. ☠

Other Notable Events 🔍

- Multiple AWS security group modification alerts on

Ask me anything from 'summarize this alert' to 'help me build a query...'

User

SYSTEM — Related hosts: 1

User information

User ID S-1-5-18	**First seen** Aug 1, 2022 @ 13:05:35.762	**Operating system** Windows, +1 More
Domain NT AUTHORITY	**Last seen** 35 seconds ago	**Family** windows
Max anomaly score by job —		**IP addresses** 10.132.15.235, +3 More
User risk score 97	**User risk classification** ● Critical	

Related hosts

Name	Ip addresses	Host risk classification
bhusa-windows-2	10.132.15.235, +3 More	● Critical

Highlighted fields

Field	Value
host.name	bhusa-windows-2
agent.status	Unhealthy
user.name	SYSTEM
process.executable	C:\Windows\System32\msiexec.exe

Insights

Entities

SYSTEM

Domain NT AUTHORITY	**User risk classification** ● Critical

bhusa-windows-2

Family windows	**Host risk classification** ● Critical

telligence

ted fields for this alert were observed

You at: 8/30/2023, 7:55:23 AM

As an expert user of Elastic Security, please generate an accurate and valid EQL query to detect the use case below. Your response should be formatted to be able to use immediately in an Elastic Security timeline or detection rule. If Elastic Security already has a prebuilt rule for the use case, or a similar one, please provide a link to it and describe it.

Data exfiltration on linux systems

Assistant at: 8/30/2023, 7:55:47 AM

To create an EQL query targeting data exfiltration on Linux systems, you can look for Linux processes making a high number of DNS requests and transferring a large amount of data over the network, which might indicate data exfiltration. Here's an EQL query to help you with this:

```
sequence by process.entity_id
  [ network where process.name : "dig" and
             destination.domain not in ("*.trusted_domain.com")
  ]
  [ network where (destination.bytes > 10485760 or source.bytes > 10485760) and
             destination.port not in (80,443) and source.port not in (80,443)
  ]
```

elastic

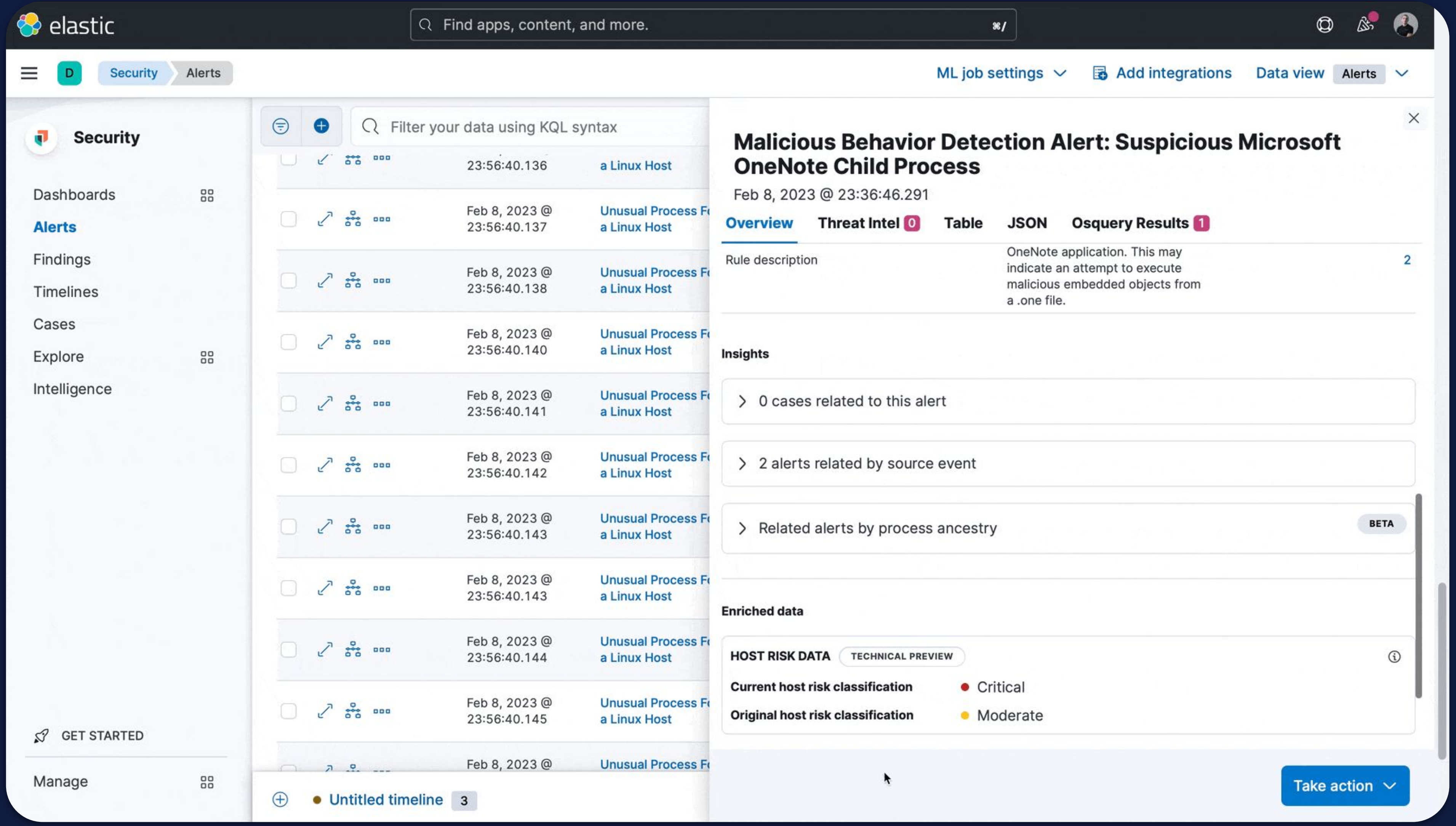
Arm every analyst

Protect → **Investigate** → **Respond**

Prevent and detect threats at the outset

Streamline investigation

Remediate the threat in the same workflow



23:56:40.136 a Linux Host
Feb 8, 2023 @ 23:56:40.137 Unusual Process F a Linux Host
Feb 8, 2023 @ 23:56:40.138 Unusual Process F a Linux Host
Feb 8, 2023 @ 23:56:40.140 Unusual Process F a Linux Host
Feb 8, 2023 @ 23:56:40.141 Unusual Process F a Linux Host
Feb 8, 2023 @ 23:56:40.142 Unusual Process F a Linux Host
Feb 8, 2023 @ 23:56:40.143 Unusual Process F a Linux Host
Feb 8, 2023 @ 23:56:40.143 Unusual Process F a Linux Host
Feb 8, 2023 @ 23:56:40.144 Unusual Process F a Linux Host
Feb 8, 2023 @ 23:56:40.145 Unusual Process F a Linux Host
Feb 8, 2023 @ Unusual Process F

Malicious Behavior Detection Alert: Suspicious Microsoft OneNote Child Process

Feb 8, 2023 @ 23:36:46.291

Rule description OneNote application. This may indicate an attempt to execute malicious embedded objects from a .one file. 2

Insights

- 0 cases related to this alert
- 2 alerts related by source event
- Related alerts by process ancestry BETA

Enriched data

HOST RISK DATA TECHNICAL PREVIEW

Current host risk classification ● Critical

Original host risk classification ● Moderate elastic security labs

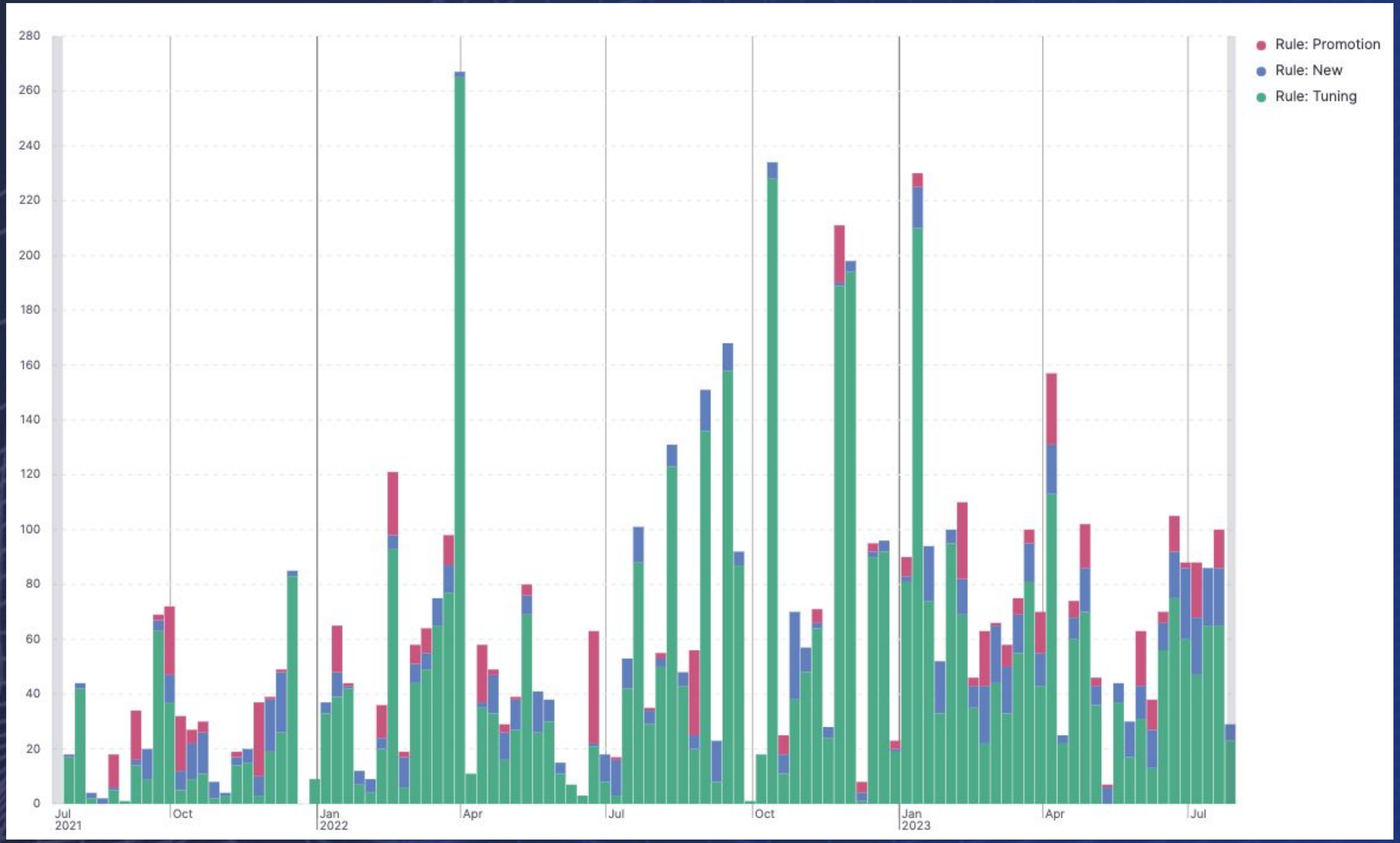
First-party threat research drives:

- Ongoing detection rule and machine learning model updates & data driven product enhancements
- Curated security artifacts for malware, ransomware, memory threats, and more
- Lower the analyst learning curve with triage and investigation guides

Check out the 2023 Global Threat Report:

https://www.elastic.co/gtr

Security artifact updates (7/2021 - 7/2023)



New Rules: 348

Promoted Rules: 349

Tuned Rules: 1669

Focus on solving for data

Optimize resources

Centralize operations

Arm every analyst

Accelerate workflows

Improve posture

Thank You

elastic | The Search Analytics Company