

Modernisieren von SecOps mit Elastic Security

Dalibor Galić - Enterprise Account Executive

Matthias Holzgethan - Senior Solutions Architect



Meet Elastic

Elastic helps everyone find answers that matter.
From all data. In real time. At scale.



Founded in 2012



2800+
employees



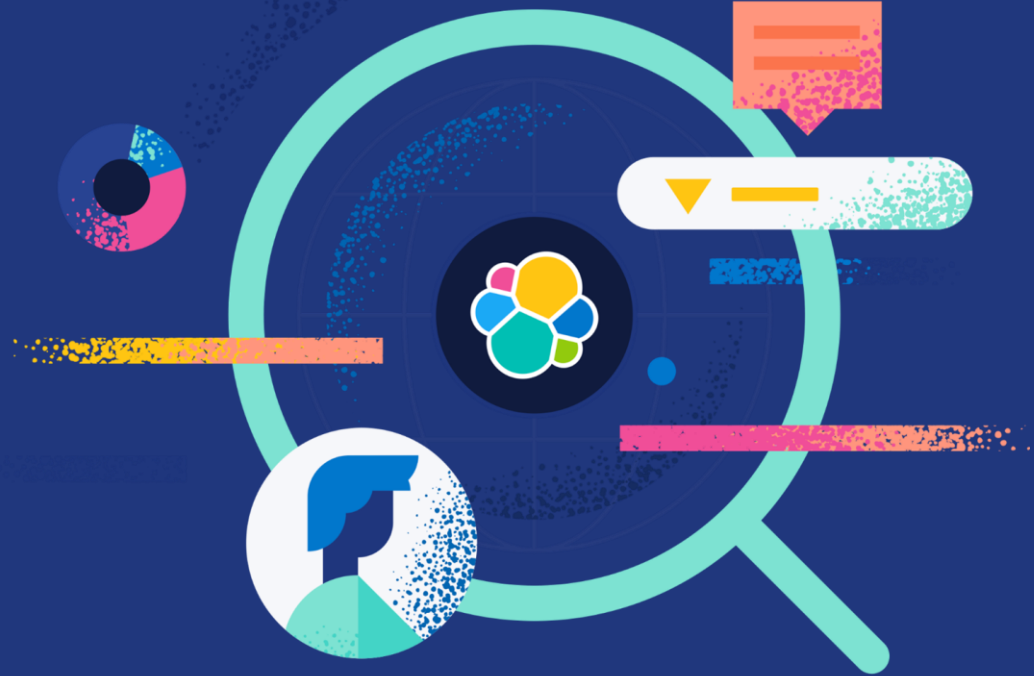
40+
Countries with employees



4B+
downloads



54%
Of Fortune 500 companies
trust Elastic



One **Data** Analytics Platform Two Out-of-the-Box Solutions The Freedom to Build Anything



Elastic is Wherever Your Data Lives



Public Cloud



Hybrid



On-Premises



Google Cloud



Alibaba Cloud



Tencent Cloud



Amazon Web Services



Google Cloud



Microsoft Azure

50+ Cloud Regions Globally



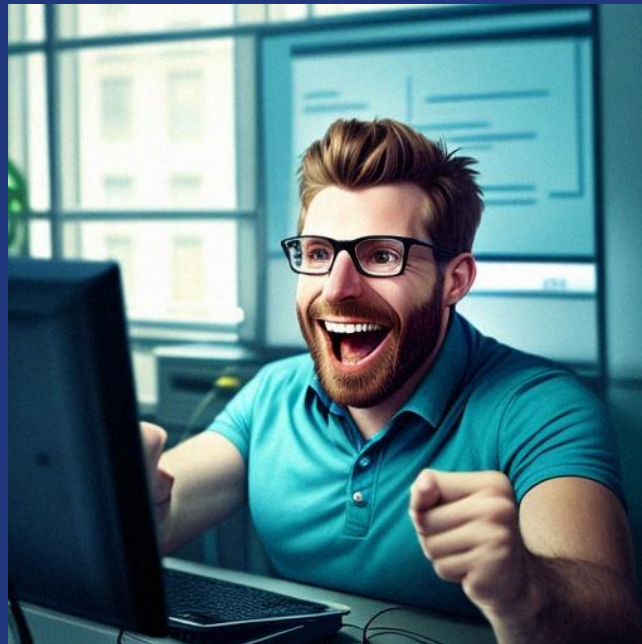


SIEM Installationen und Migrationen stellen Unternehmen vor große Herausforderungen

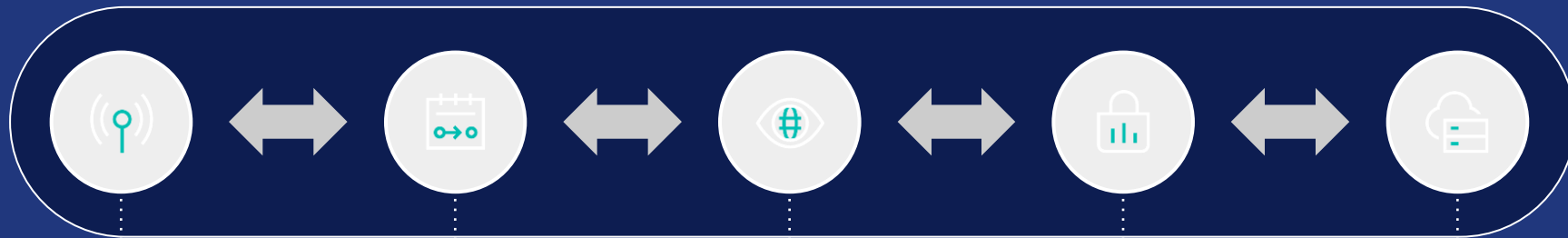


... hilft dabei Risiken zu reduzieren und das Budget zu optimieren:

- **Dynamische Security Workflows helfen den Security Analysten**
- **Security Ausgaben können durch die flexiblen Lizenz-Optionen optimiert werden**
- **Zukunftssicherheit für Ihr SOC durch kontinuierliche Innovation**



Typische Herausforderungen im Bereich Security



Zu viele Alarme

Security-Teams werden mit Alarmen "geflutet" - die wirklichen Vorfälle können dabei untergehen

Zu langsame Reaktion

Oft fehlt der Kontext zu einem Alarm. Dies erschwert die korrekte Einstufung von Alarmen und verzögert die korrekte Reaktion

Eingeschränkte Sicht

Silos, Skalierungs- und Kostenprobleme schränken die Transparenz ein und verlangsamen die Erkennung von Vorfällen

Geringe Flexibilität

SIEM, Endpoint und Cloud tools sind oft nicht flexible genug und um Kosten zu sparen wird dann oft nicht das gesamte Unternehmen abgedeckt

Komplexität in der Cloud

Hohe Kosten für Datentransfer und Datenhoheit sowie eine sehr dynamische und schnell wachsende Umgebung



Zukunftssicherheit für Ihr SOC

On prem



Containerized



Cloud



Multi Cloud



Hybrid



Custom Dashboards



Graph Analysis



Machine Learning



Maps



Canvas Presentations

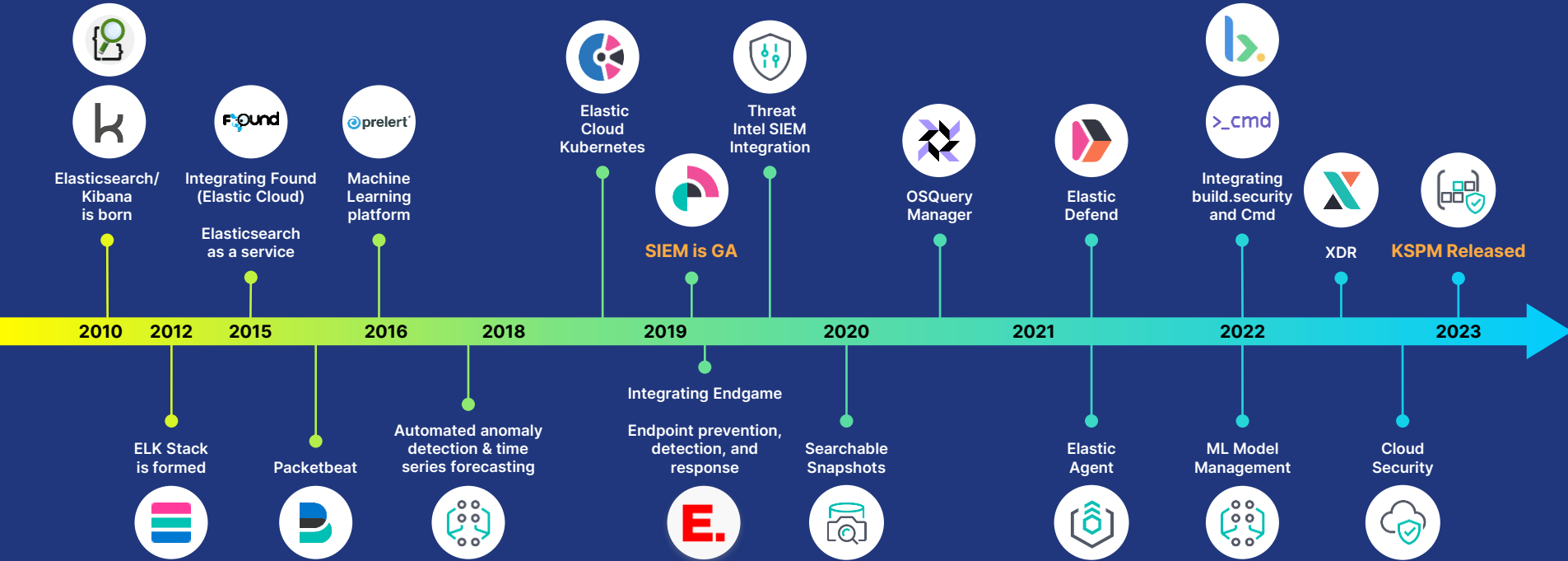


Open Source Community



Zukunftssicherheit für Ihr SOC

Nachweisliche Erfolgsbilanz in Sachen Innovation



Bring your data

Detect, Investigate & Respond

cloud



network



host



user



email



threat intel



Native protection

Block threats with Elastic Agent

laptops & desktops



servers & VM's



containers & kubernetes



cloud providers



Elastic Security

SIEM & Security Analytics

Endpoint Security

Cloud Security

Powered by Elastic Security Labs - Threat Research



Das Werkzeug für Security Analysten

Protect



Investigate



Respond



Angriffe erkennen
bevor diese starten



Automatisierung beim
Threat Hunting



Bedrohungen (im
gleichen Workflow)
erfolgreich abwehren

Process Name	Timestamp
CHROME.exe	Feb 5, 2023 @ 23:42:09.432
ANALYSIS.exe	Feb 5, 2023 @ 23:42:40.289
mofmap.exe	Feb 5, 2023 @ 23:42:49.425
curl.exe	Feb 5, 2023 @ 23:43:00.592
runRSE2.exe	Feb 5, 2023 @ 23:42:45.695
cmd.exe	Feb 5, 2023 @ 23:43:04.752
net.exe	Feb 5, 2023 @ 23:50:11.047
ADP.exe	Feb 5, 2023 @ 23:50:23.476
ipconfig.exe	Feb 5, 2023 @ 23:50:23.628
mshta.exe	Feb 5, 2023 @ 23:50:23.849
cmd.exe	Feb 5, 2023 @ 23:50:23.115



Das Werkzeug für Security Analysten

Protect



Investigate



Respond



Angriffe erkennen
bevor diese starten



Automatisierung beim
Threat Hunting



Bedrohungen (im
gleichen Workflow)
erfolgreich abwehren

The screenshot shows the Elastic Security console. On the left is a navigation menu with 'Security Alerts' selected. The main area displays a list of alerts. The top alert is a 'Malicious Behavior Detection Alert: Suspicious Microsoft OneNote Child Process' from Feb 8, 2023, at 23:36:46.291. Below it is a detailed view of this alert, showing a process event where 'onenote.exe' started a child process 'onenote.exe'. The alert is categorized as 'high' and includes a 'Guided' link for more information. Other alerts in the list include 'Unusual Process for a Linux Host' and 'New Process Executed by Microsoft OneNote'.



Das Werkzeug für Security Analysten

Protect



Investigate



Respond



Angriffe erkennen
bevor diese starten



Automatisierung beim
Threat Hunting



Bedrohungen (im
gleichen Workflow)
erfolgreich abwehren

The screenshot shows the Elastic Security console. The main alert is titled "Malicious Behavior Detection Alert: Suspicious Microsoft OneNote Child Process" and occurred on Feb 8, 2023 at 23:36:46.291. The alert details include a rule description, insights (0 cases, 2 alerts, and related alerts by process ancestry), and enriched data. The enriched data shows a "Current host risk classification" of "Critical" and an "Original host risk classification" of "Moderate". A "Take action" button is visible at the bottom right of the alert details.



Optimierung der Security-Ausgaben

Trotz hoher Aufbewahrungsdauer und hoher Verfügbarkeit

Konsolidierung

Optimiertes Budget

- SIEM
- Endpoint
- Cloud
- Container
- Soar
- Threat Intel
- Observability



Hot
\$\$\$ / GB
"SOFORT!"



Warm
\$\$ / GB
"In einer Sekunde"



Cold
\$ / GB
"In einer Minute"



Frozen
\$ / GB
"In Minuten"

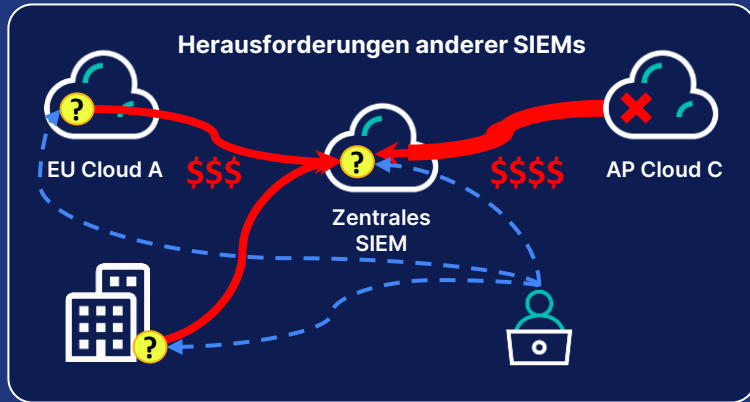
Automatisierte Verwaltung der "Data Tiers"

100% live und durchsuchbar in allen "Data Tiers"



Optimierung der Security-Ausgaben

Hohe Flexibilität in hybriden und Multi-Cloud Umgebungen

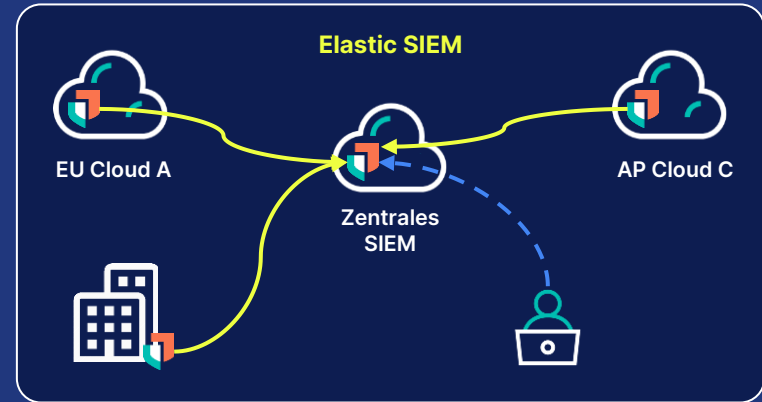


Cloud Kosten

- Datentransferkosten sind hoch

Komplexität in hybriden Cloud-Umgebungen

- Gleiche Funktionen?
- Wo sind meine Daten gespeichert?
- Verfügbarkeit der Cloud-Umgebungen?



Datenzugriff leicht gemacht

- Sicheres "Distributed Search"
 - Korrelation zwischen Cloud Instanzen
 - Datenhoheit sicherstellen
 - Vollständiges RBAC / ABAC
 - Datentransferkosten deutlich reduzieren
- Gleicher Funktionsumfang zwischen Cloud und self-managed
- 50+ Elastic Cloud Regionen

Integrationen mit wichtigen Partnern



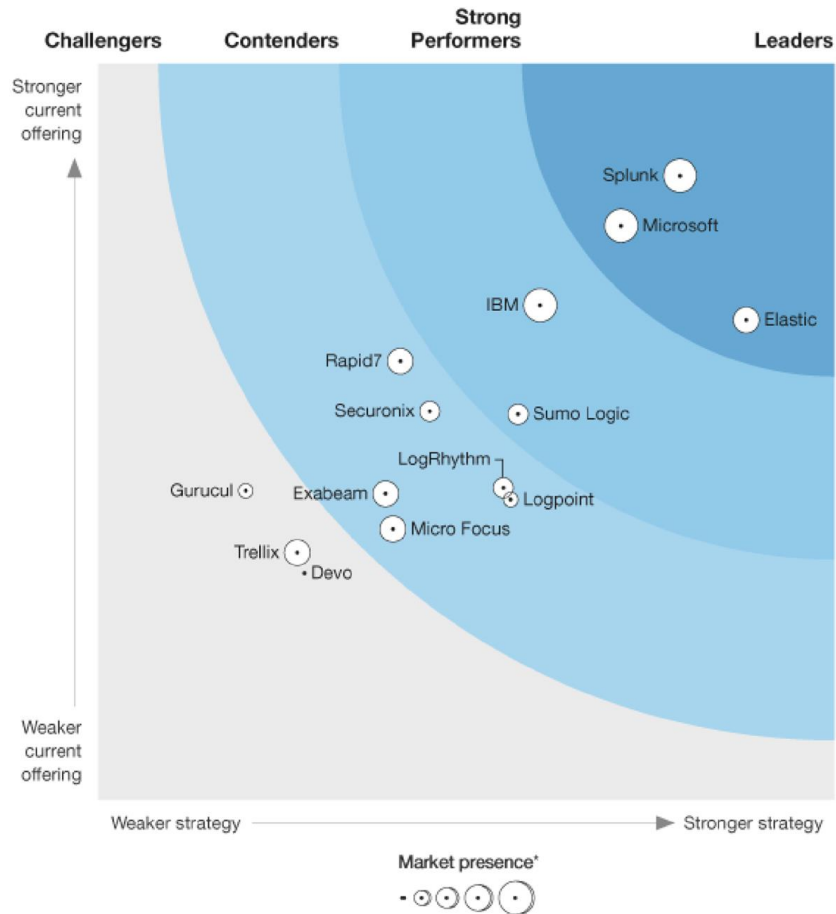
Elastic named a Leader in The Forrester Wave™ Security Analytics Platforms Q4 2022



- *“Elastic provides incredible flexibility and visualizations in an open offering.”*
- *“Reference customers value the flexibility on pricing and subsequent cost savings that Elastic provides.”*
- *“Elastic Security best suits clients comfortable with security engineering looking for an extremely customizable product.”*

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester New Wave™ is a graphical representation of Forrester’s call on a market. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

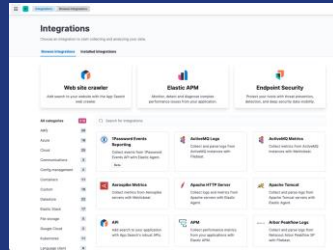
THE FORRESTER WAVE™ Security Analytics Platforms Q4 2022



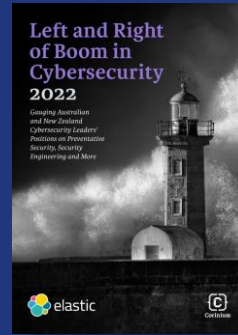
Wie können Sie mehr über Elastic Security erfahren?



Elastic's Research (z.B. Global Threat Report) ist verfügbar via Security Labs elastic.co/security-labs



Elastic Security selbst ausprobieren cloud.elastic.co



Lesen sie unser Paper "Left and Right of Boom in Cybersecurity" elastic.co/left-right-boom-cybersecurity-2022

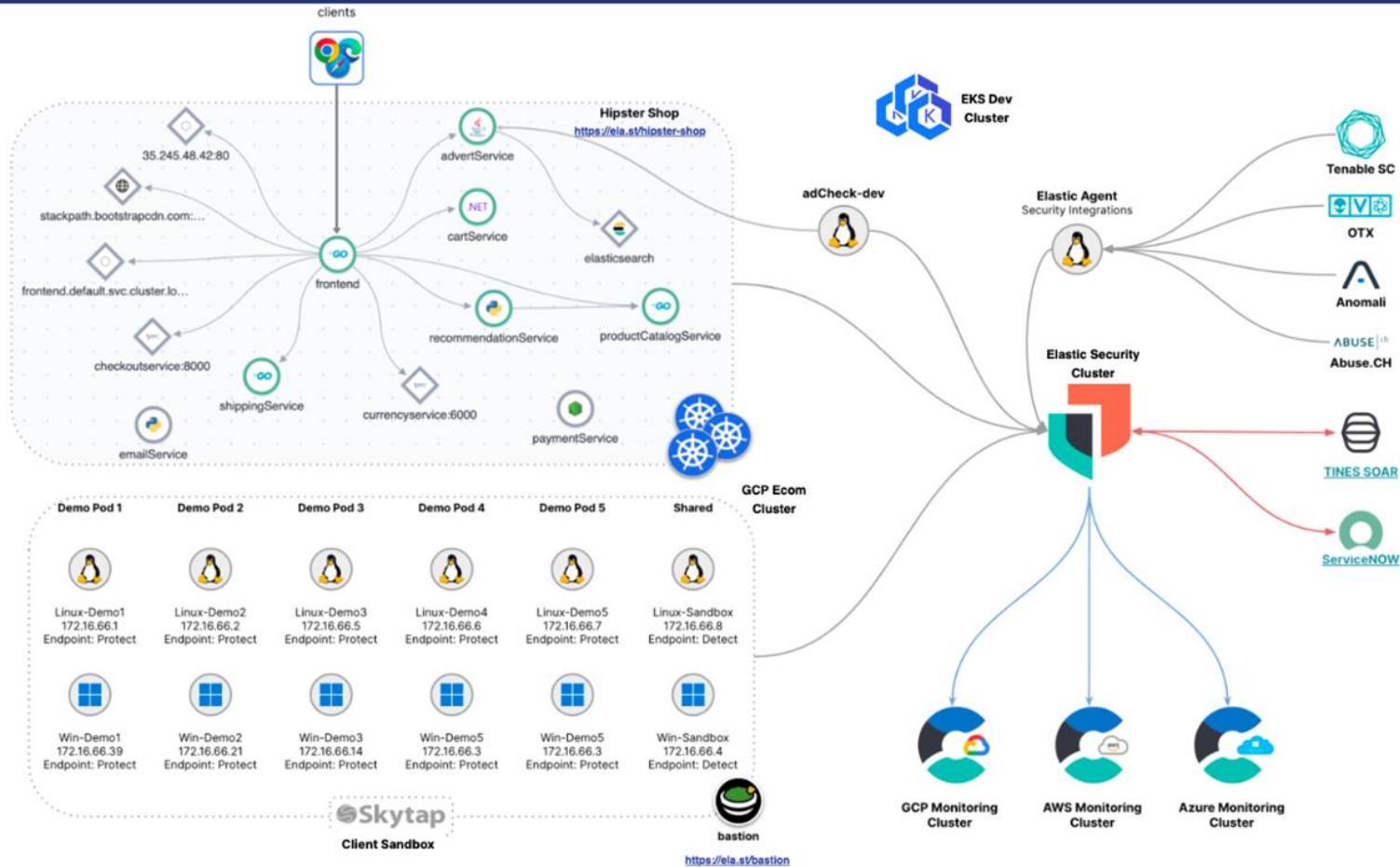


Schauen Sie sich eine Malware Demo an ohmymalware.com



Sprechen Sie mit Ihrem Elastic Account Team

Demo



**Vielen Dank für die
Aufmerksamkeit**