Predict the next step
Stop the attackers

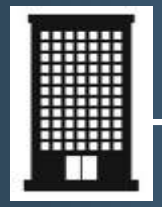
Raffaele Clementelli – Country Manager DACH & Italy

October 2022

ANOMALI

Anomali

Founded in 2013 by the “Father of SIEM” - Hugh Njemanze



Global HQ in Redwood City, USA
European HQ in Belfast, Ireland

Largest repository of curated Threat Intelligence in the World

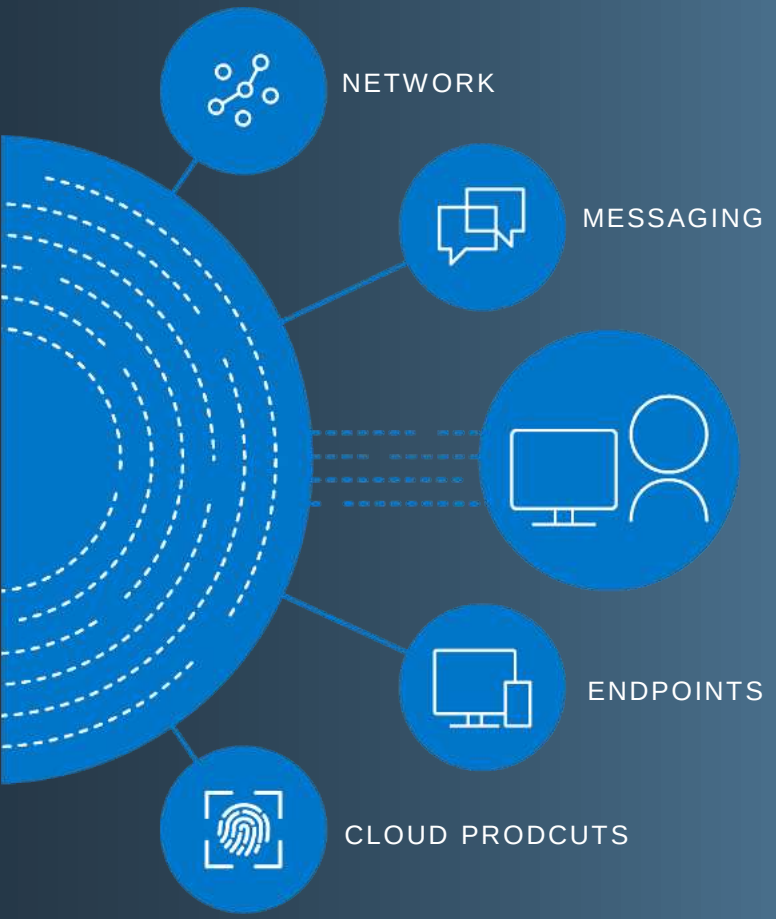
600+ Customers Worldwide

200+ Native Integrations
Partnerships / Tech alliances

Customer Success Manager
Included with every Anomali subscription

Establishing cyber resilience is challenging

LOCAL TELEMETRY



Silo-ed Security Organization

Lack of global threat visibility impedes digital transformation

Fatigued staff overburdened with low fidelity signals

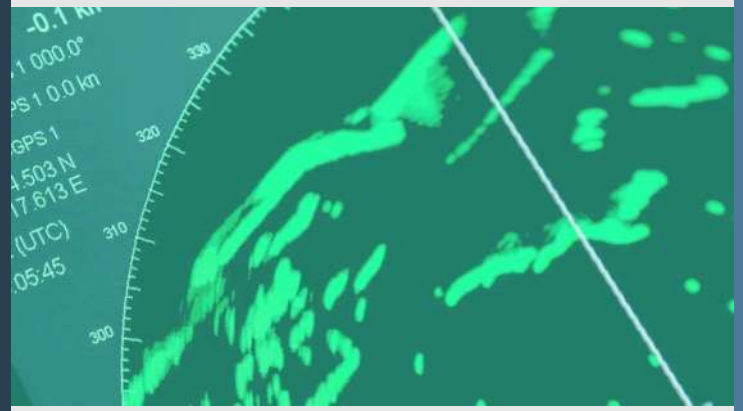
Investments wasted across an uncoordinated response

GLOBAL THREAT INTELLIGENCE

ANOMALI

What if you could…stop the attack and predict the next one?

UNLIMITED VISIBILITY



- Look across all relevant telemetry and data silos.
- Enhance the efficacy of your existing investments.
- Have greater visibility into how global threats impact your organization.

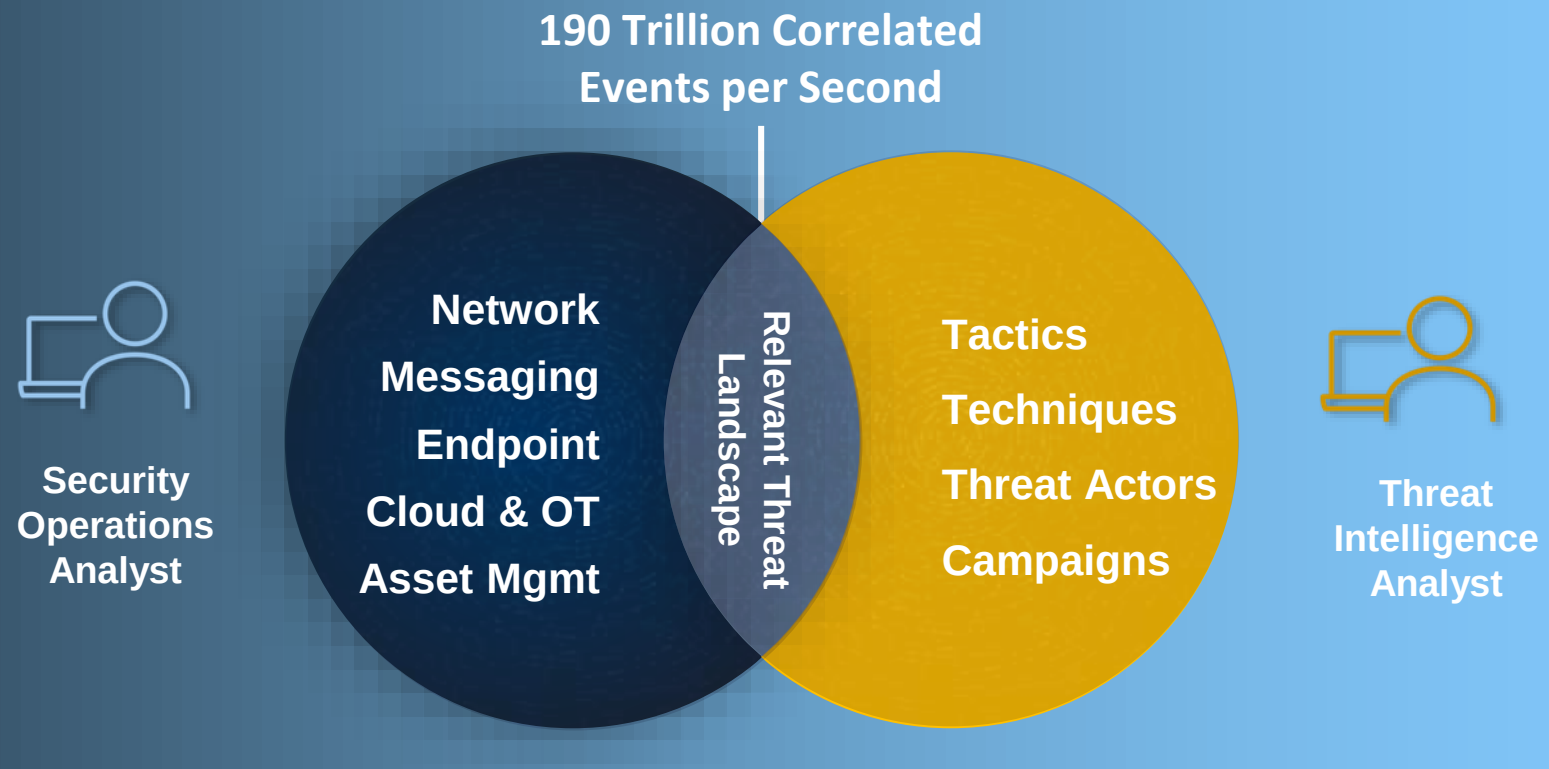
PRECISION DETECTION

- Leverage ALL of the threat intelligence.
- Overcome the limitations of the tools in your security stack.
- Empower your team to focus on real threats and reduce false positives.

EFFECTIVE RESPONSE

- Leverage machine learning and automation to increase productivity and efficiency of your teams.
- Continuously monitor for new globally identified threats - going back 5+ years.

We not only stop the breach. We stop the attackers.



Continuous Detection | Retrospective Detection | Attack Pattern Detection

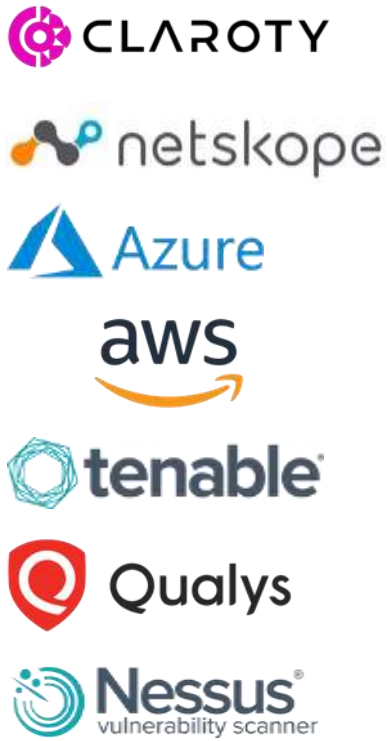
Open Platform with Native Integrations for Telemetry

Network

SIEM

Endpoint

Other



..and more custom integrations!

Intelligence based Platform: 130+ Feeds, Enrichments, Tools

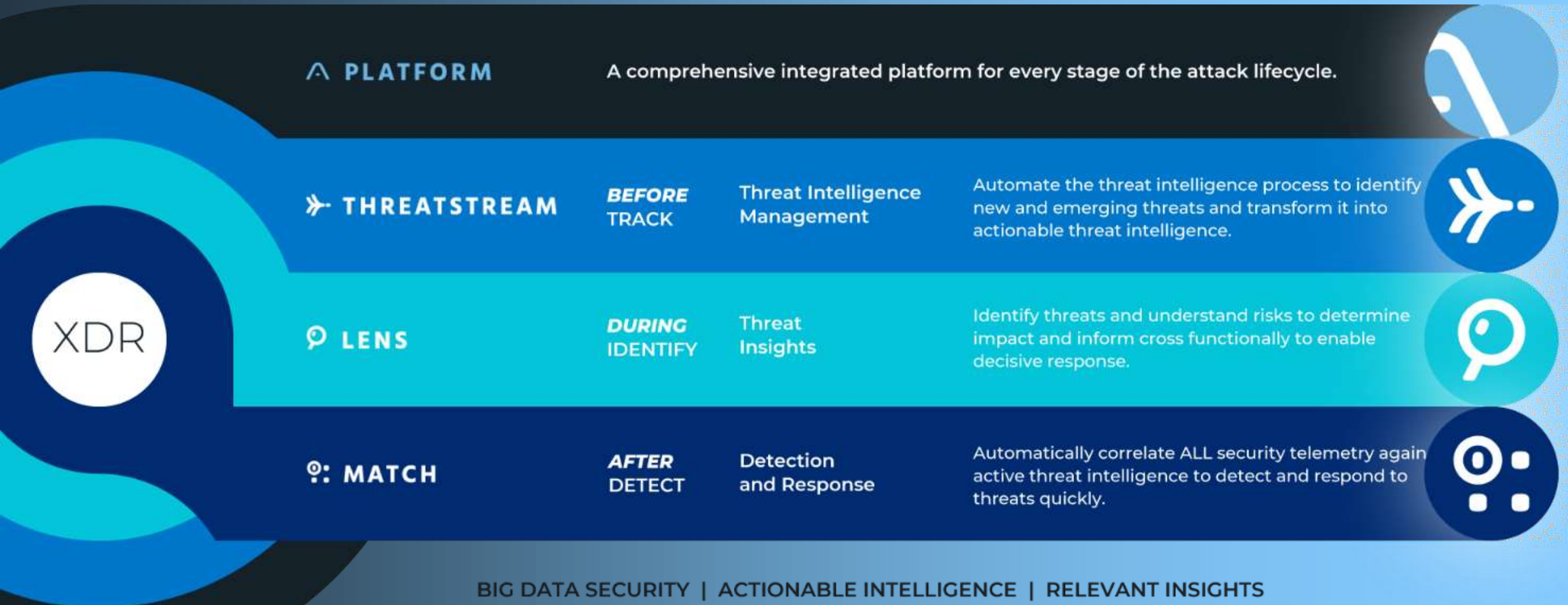
Feeds

Enrichments

Integrations

Tools

The Anomali Platform – Cloud and On-Prem

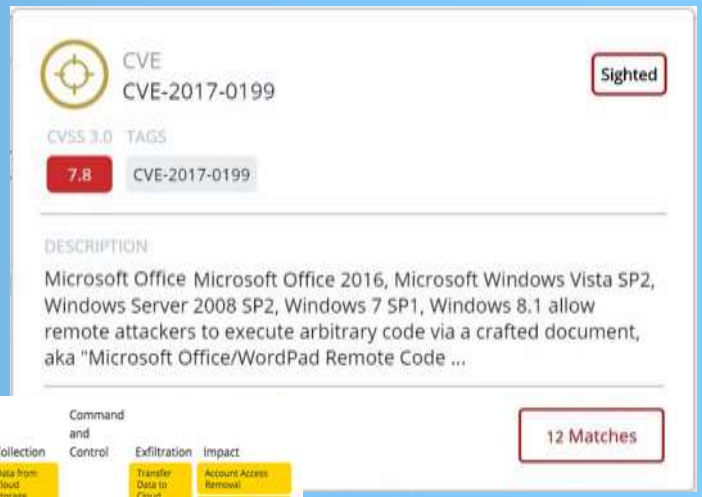


ANOMALI

Accelerate Threat Hunting

- Real-time search by IOC, actor, threat bulletin
- Scan, analyze and import new Intelligence
- MITRE ATT&CK context
- MITRE ATT&CK next step prediction
- Predictive DGA domains
- Predictive attack patterns

Anomali Lens:
Scan new threats, research and find matches in your environment in real time.



MITRE ATT&CK:
Research TTPs associated with a threat actor.

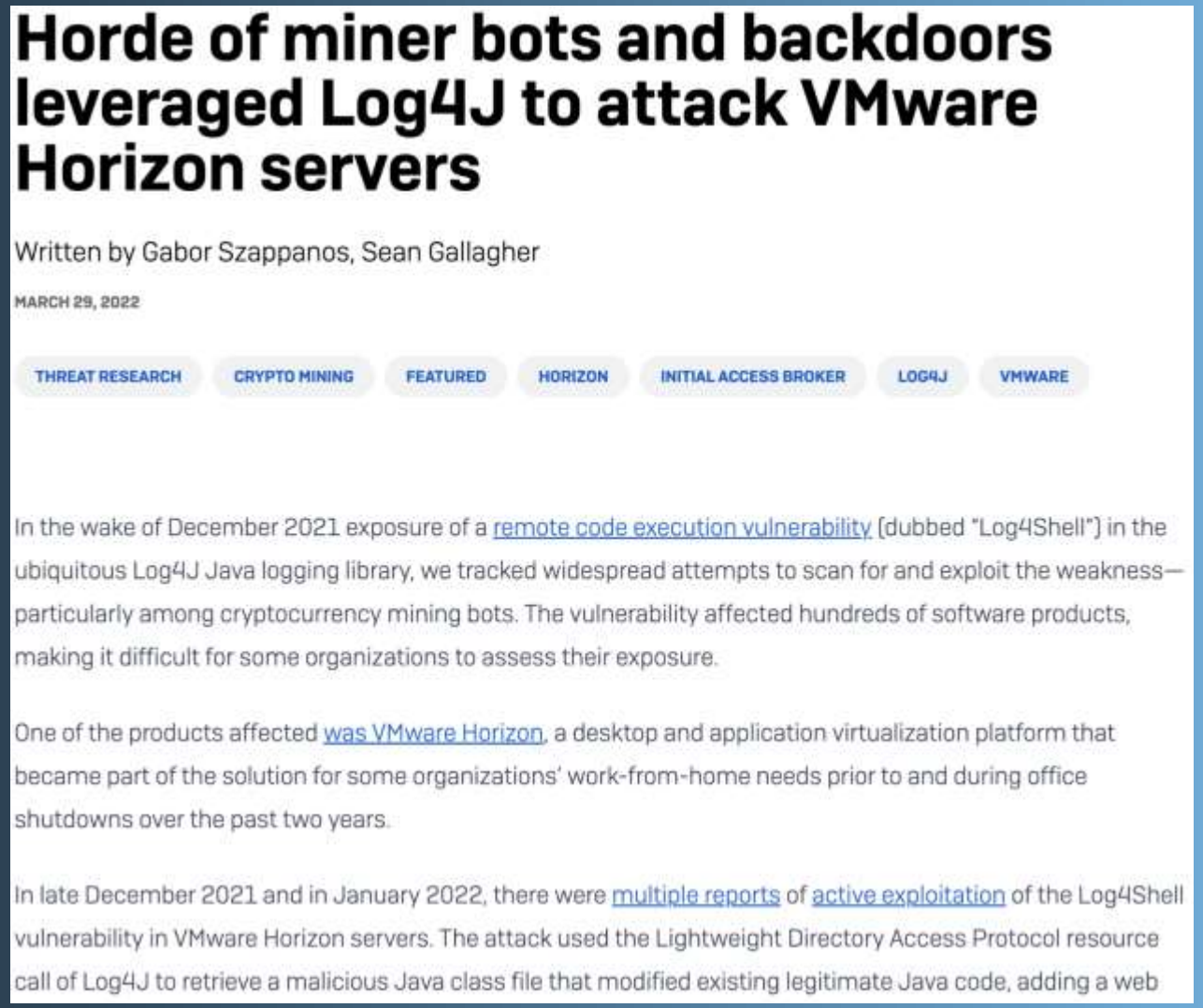
Explorer:
Visually enrich, expand and pivot on threat indicators.

Anomali Digital Risk Protection

- **Cost efficient, Comprehensive, High-quality** Targeted Threat Monitoring Service provided by Anomali's Threat Research Team.
- **Digital Risk Proection Dashboards & Alerting** Real-time, automated updated dashboards in your ThreatStream.

Alert Type
Domain Hijacking
Rogue Apps
Employee Doxing Incidents
Pastebin Brand Mentions
Leaked Documents
Leaked Code Monitor
Trademark Application Filing
E-mail Vulnerability
SSL Certificate Validity
Leaked Employee Emails

New Exploit Announced
Answering “Have we been affected?” **without** Anomali



Horde of miner bots and backdoors leveraged Log4J to attack VMware Horizon servers

Written by Gabor Szappanos, Sean Gallagher

MARCH 29, 2022

THREAT RESEARCH | CRYPTO MINING | FEATURED | HORIZON | INITIAL ACCESS BROKER | LOG4J | VMWARE

In the wake of December 2021 exposure of a remote code execution vulnerability (dubbed “Log4Shell”) in the ubiquitous Log4J Java logging library, we tracked widespread attempts to scan for and exploit the weakness—particularly among cryptocurrency mining bots. The vulnerability affected hundreds of software products, making it difficult for some organizations to assess their exposure.

One of the products affected was VMware Horizon, a desktop and application virtualization platform that became part of the solution for some organizations’ work-from-home needs prior to and during office shutdowns over the past two years.

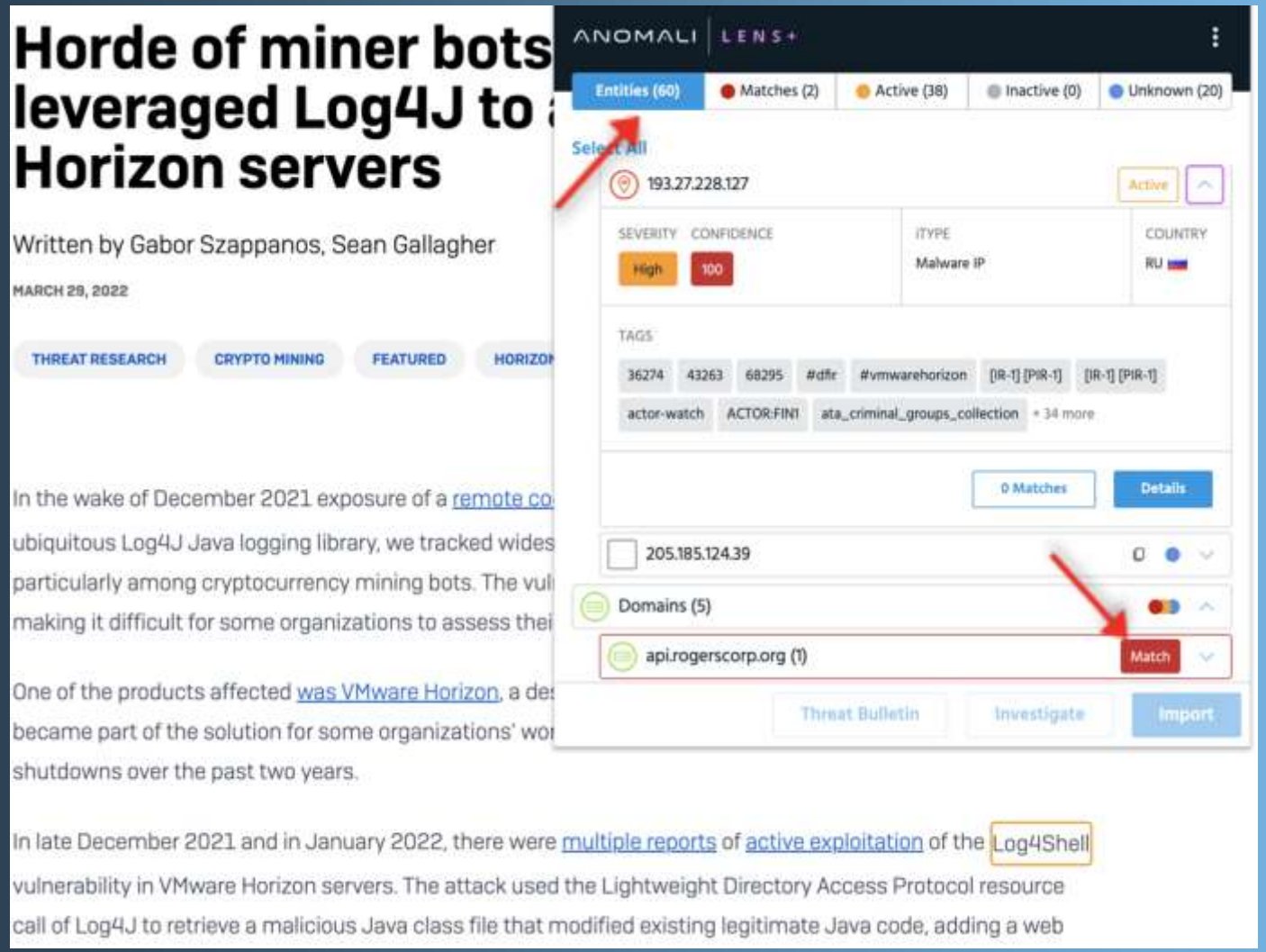
In late December 2021 and in January 2022, there were multiple reports of active exploitation of the Log4Shell vulnerability in VMware Horizon servers. The attack used the Lightweight Directory Access Protocol resource call of Log4J to retrieve a malicious Java class file that modified existing legitimate Java code, adding a web

- CISO sends you a security blog about a new threat – “Are we affected?”
- Skim article and identify known and unknown security terms
- Research unrecognized threat actors, malware families, vulnerabilities, etc.
- Extract and validate indicators of compromise
- Correlate indicators with network logs to identify if this has ever been seen in your environment for **past 1 year…**

ELAPSED TIME: 1-2 WEEKS

ANOMALI

New Exploit Announced
Answering “Have we been affected?” **with** Anomali

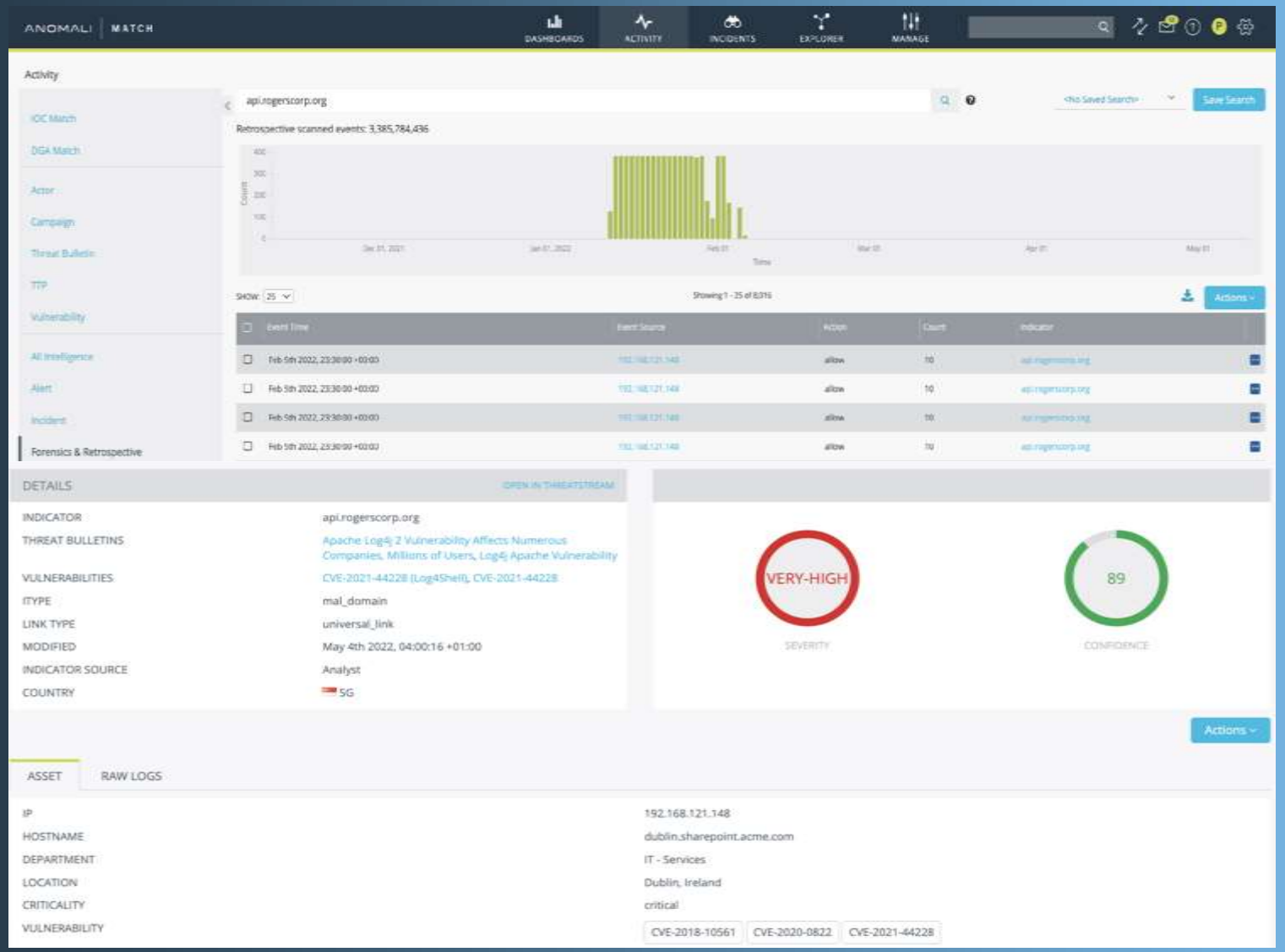


- CISO sends you a security blog about a new threat – “Are we affected?”
- Lens immediately highlights the presence of the threat

ELAPSED TIME: 15 SECONDS

Happens automatically with continuous intelligence that alerts on relevant threats

Answering “Have I been attacked?” **with** Anomali



- Pivot at the click of a button to the retrospective threat hunt displayed in Match
- Review details of affected assets to perform mitigation steps

ELAPSED TIME: 15 SECONDS

Recall relevant correlation events with a click of one menu button

Why Anomali

Extended Visibility

- Collection of ALL security telemetry at scale
- Correlation of ALL global intelligence
- Quick scan and import of new intelligence

Precision attack Detection

- Continuous global attack detection
- Retrospective forensic detection up to 5 Years
- Attack Pattern Detection
- Next attack phase prediction

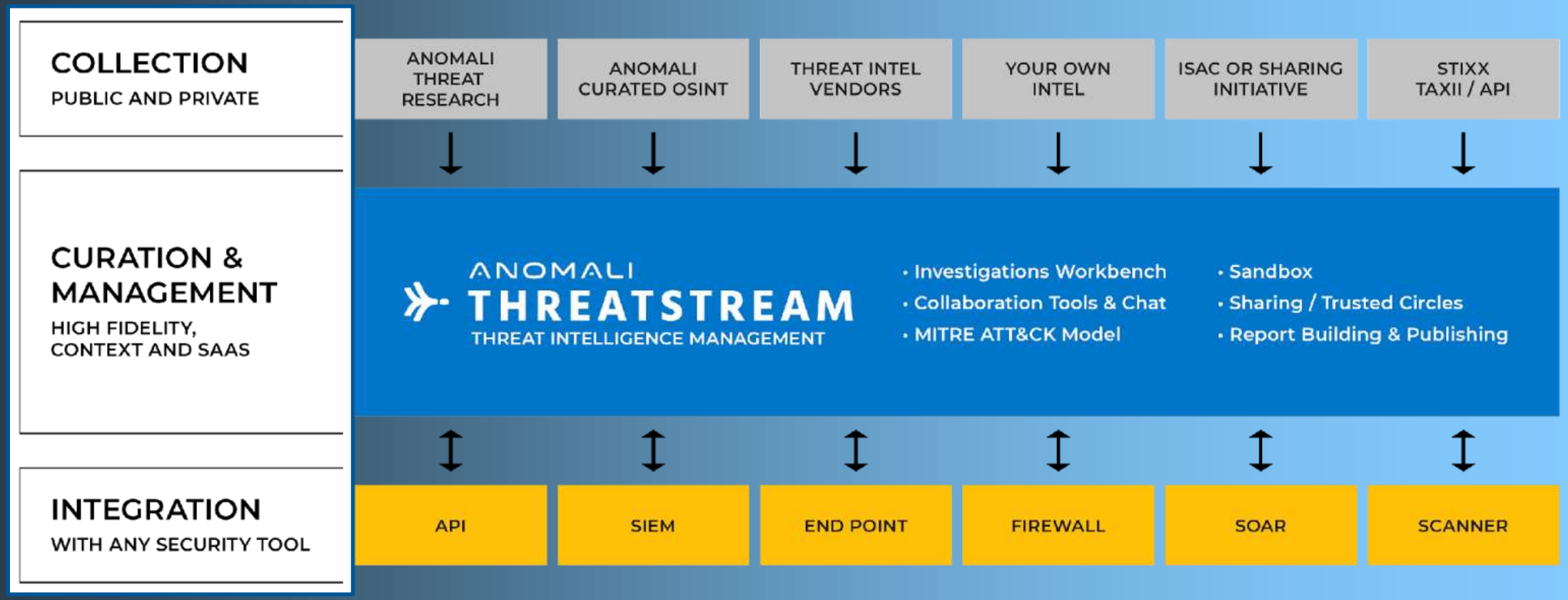
Effective Response

- Automated root-cause analysis
- Intelligence prioritized response
- Integration with 50+ security controls

Thank you

ThreatStream Overview

- Automate the collection of threat data and intelligence at scale, from thousands of sources and feeds
- Automate the curation of the data and intelligence, normalized, de-duplicated, enriched, confidence scored
- Automate the operationalizing of threat intelligence, through integrations with security tools/controls



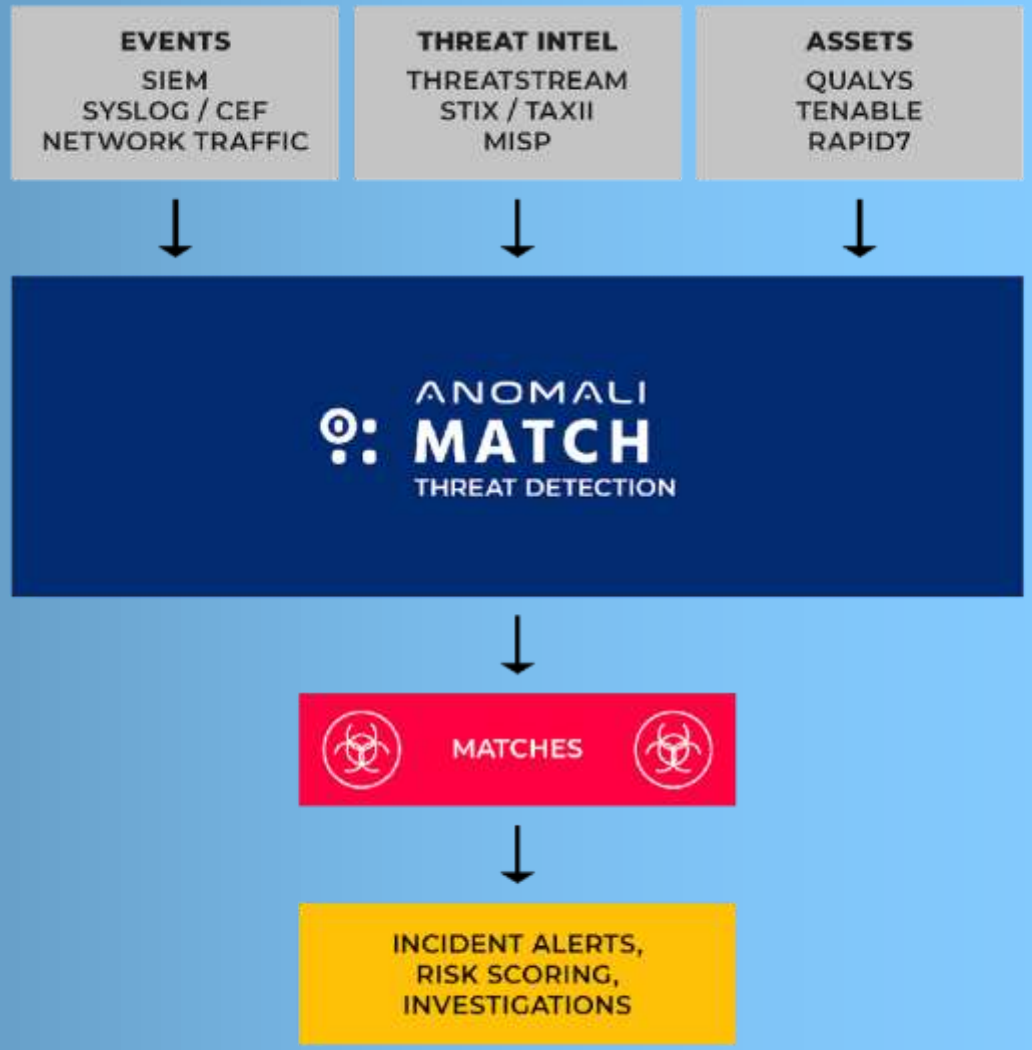
Match Overview

Detect relevant threats — pinpoint relevant threat activity on your network in real-time to reduce threat dwell times

Research and prioritize alerts — view alerts enriched with threat intelligence context, asset criticality, and risk scores

Hunt for threats — accelerate and scale threat hunting activities with real-time search and TTP-based hunting

Retrospective search — automated retrospective search to find previously hidden incursions and review a timeline of compromise



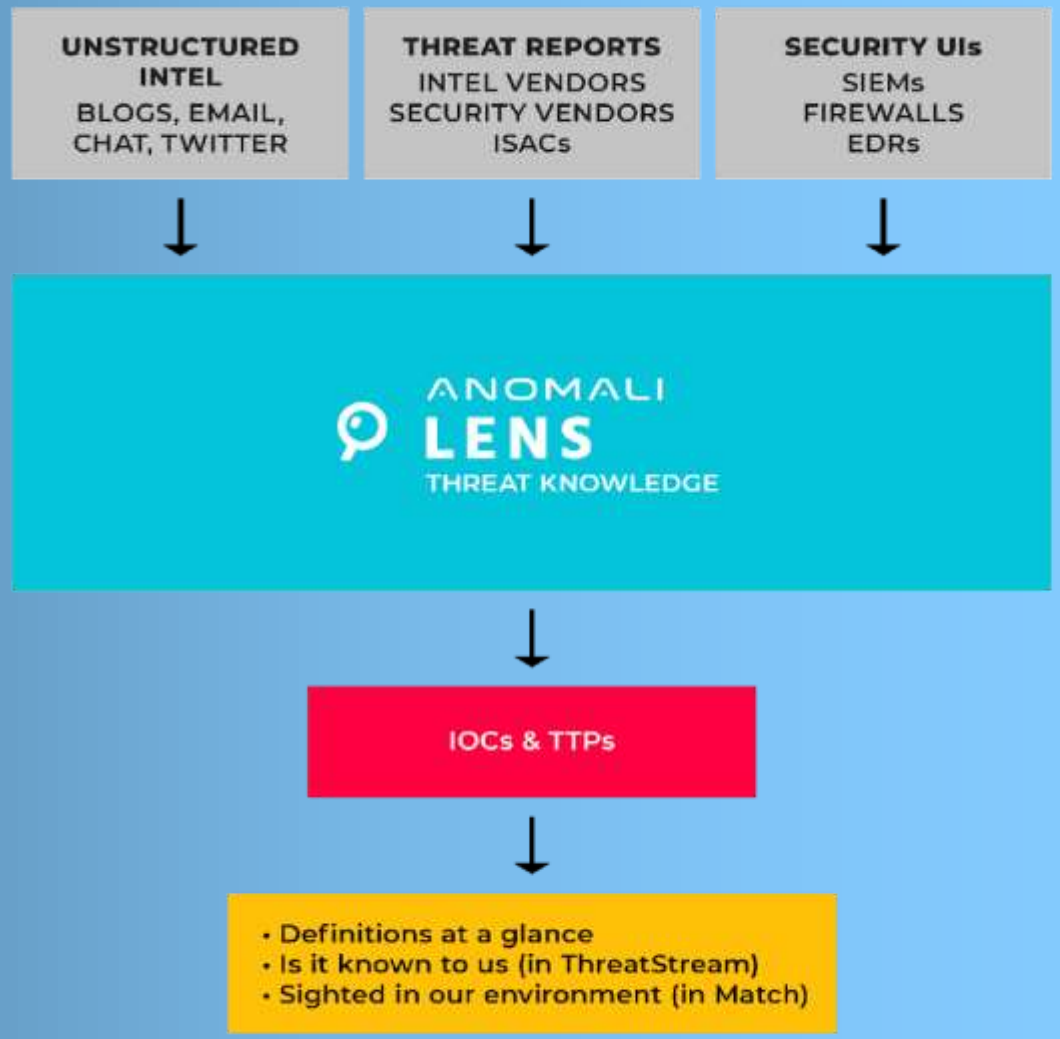
Lens+ Overview

Uncover intelligence within unstructured data — scan Office 365, PDF's and web-based content to unveil relevant intelligence in seconds

Identify threats automatically — automate identification of threat indicators and activity with Natural Language Processing (NLP)

Transform data into actionable intelligence — associate content with MITRE ATT&CK IDs and instantly export to a ThreatStream Investigation

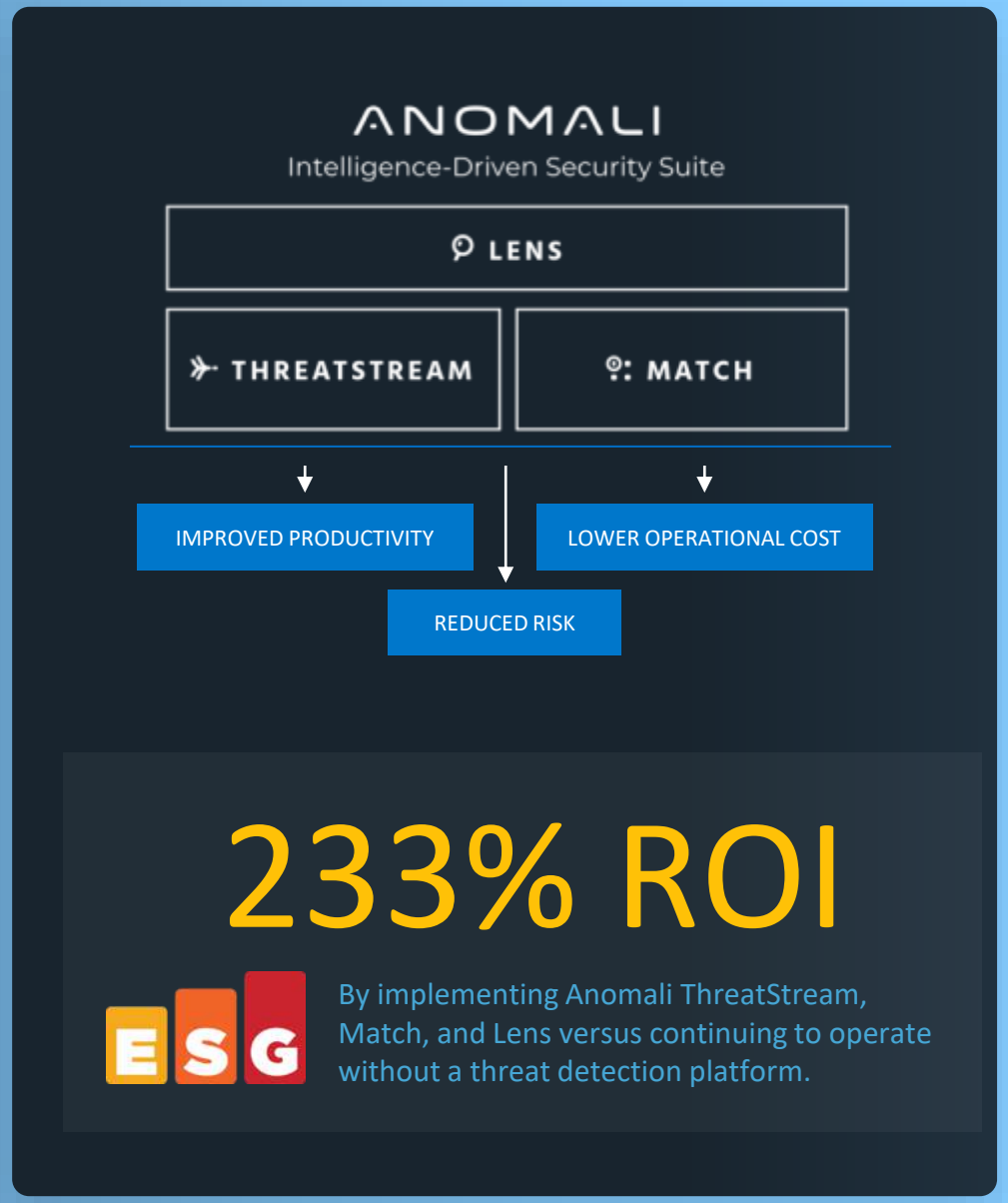
Create threat bulletins — distribute in-depth reports to inform threat detection, response, and remediation efforts as well as



Intelligence Based Open XDR

Proof Points: Anomali in Action

- **Monitor cybersecurity risks, detect potential attacks, and identify gaps in security coverage.**
- **Prevent interruptions of critical business processes with accurate, high-fidelity intelligence.**
- **Make fast decisions and automatically respond when under attack.**



233% ROI

ESG

By implementing Anomali ThreatStream, Match, and Lens versus continuing to operate without a threat detection platform.

Use cases

Use Case	Description
Driving Informed Decisions	Make security informed decision that impact efficacy and efficiency using detection, context and industry benchmarking insights. .
Continuous Intel Monitoring	Continuously monitor threat landscape for IOCs and associated threat models to enable quick and effective response.
Pinpoint Relevant Threats	Quickly profile threat and impact on. understand criticality and prioritize response efforts.
Predict the Next Attack	Use MITRE ATT&CK based pattern analysis to strengthen your security posture, preventing future attacks.
Accelerate Threat Hunting	Scale hunting with intel-based search, increasing team efficiency / productivity - focusing on org relevant threats.
Elevate Strategic Intel	Move from IOC to threat actor detection providing a more comprehensive assessment of attack impact.
Protect against Malicious Domains	Identify and manage protection against malicious domains using Anomali's machine learning detection.