CHECK POINT + ELASTIC

UNLOCK SECURITY DATA INTELLIGENCE

UNLOCK SECURITY DATA INTELLIGENCE

A Tightly Integrated Threat Prevention Ecosystem

Solution Benefits

- **Prevent threats across network, cloud, mobile and endpoint:** combine prevent-first security technologies with Elasticsearch threat hunting capabilities.
- **Unifying operations and security data makes analytics and compliance easy:** actionable information streamlines identifying and responding to threats.
- **Gain real-time visibility of your security posture:** enrich security events with content from industry-leading threat prevention products.
- **Cloud-based products and services to minimize your digital risk**: Elastic makes data usable in real time and at scale.

INSIGHTS

Visibility is key to securing any organization. Security technologies protecting networks, cloud, mobile and endpoint devices are a rich source of data and work best when a threat is known. When identified, threat analysis enables remediation and prevention when data from that analysis becomes IoCs (Indicators of Compromise) and enriches your security defenses. When security and SIEM (Security Information and Event Management) technologies are tightly integrated, organizations detect threats earlier, minimizing the impact of the breach on business mission-critical functions, valuable data and reputation.

CHECK POINT AND ELASTIC SOLUTION

Together, Check Point and Elastic deliver a unique integration that leverages the rich offering of the Check Point security product portfolio and Elastic. Stated simply, Check Point Next Generation Threat Prevention technologies and Elastic provides actionable information to streamline your threat management process, reducing the time it takes to identify and respond to real threats.

Check Point security management consolidates threat visibility across your entire security infrastructure. The single management centrally correlates all types of events across all network environments, cloud services and mobile infrastructures. When a Check Point device detects a security threat, log and event data are sent to Elastic, to be further analyzed, enriched, and prioritized in order to provide clear insight into the organization's security posture at any given time.

INTEGRATED THREAT PREVENTION ECOSYSTEM

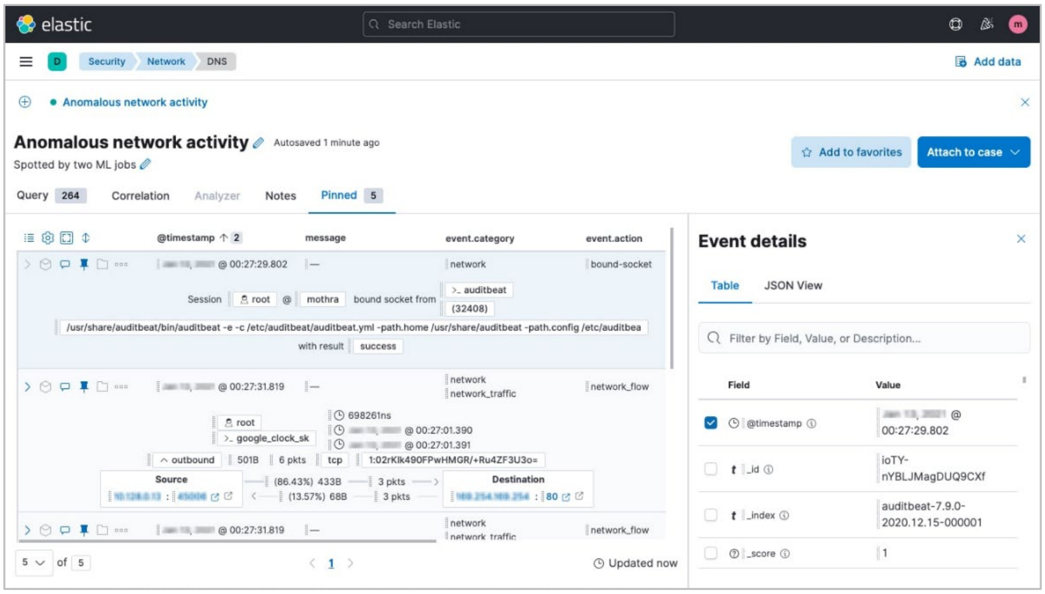
Check Point offers a fully consolidated cyber security architecture to protect your business and IT infrastructure against sophisticated cyber-attacks across networks, endpoint, cloud and mobile. Our prevention technologies stop both known and unknown zero-day attacks across all areas of the IT infrastructure, including cloud, endpoint and mobile. And if an attacker does penetrate the perimeter, we terminate command and control channels and break the cyber-attack kill chain before they can extract data. Check Point network, endpoint, cloud and mobile device log and event's data empowers Elastic SIEM analysis capabilities — identifying real threats.

UNRAVEL REAL-TIME VISIBILITY

Elastic offers three solutions for enterprise search, observability, and security, built on one technology stack that can be deployed anywhere. From finding documents to monitoring infrastructure to hunting for threats, Elastic makes data usable in real time and at scale.

- **Elastic Enterprise Search**: Millions of people choose Elasticsearch to implement powerful, modern search experiences. Use Elastic for your websites, applications, workplace content, or anything in between.
- **Elastic Observability**: Rely on the most widely deployed observability platform available, built on the proven Elastic Stack to converge silos, delivering unified visibility and actionable insights.
- **Elastic Security**: Elastic Security equips teams to prevent, detect, and respond to threats at cloud speed and scale — securing business operations with a unified, open platform.

The Check Point integration leverages Elastic Agent to ship events from Check Point Log Exporter to Elastic. The integration enables collection, analysis and correlation of Check Point events and alerts within Elastic Security. Elastic Security's out of the box detection rules, enable analysis to quickly be alerted to any suspicious traffic from your Check Point firewalls, including DNS Tunneling, unusual port activity and IOC matches against Threat Intelligence feeds. Machine learning jobs also provide visibility into abnormal spikes in denied traffic, spikes in network traffic and even network traffic to rare countries.



Anomalous network activity

Anomalous network activity Autosaved 1 minute ago

Spotted by two ML jobs

@timestamp ↑ 2	message	event.category	event.action
[redacted] @ 00:27:29.802	—	network	bound-socket
[redacted] @ 00:27:31.819	—	network network_traffic	network_flow
[redacted] @ 00:27:31.819	—	network network_traffic	network_flow

Session root @ mothra bound socket from >_ auditbeat (32408)

/usr/share/auditbeat/bin/auditbeat -e -c /etc/auditbeat/auditbeat.yml -path.home /usr/share/auditbeat -path.config /etc/auditbea

with result success

root
>_ google_clock_sk
698261ns
[redacted] @ 00:27:01.390
[redacted] @ 00:27:01.391
outbound 501B 6 pkts tcp 1:02rKlk490FPwHMGR/+Ru4ZF3U3o=

Source [redacted] : [redacted] — (86.43%) 433B — 3 pkts → Destination [redacted] : 80
← (13.57%) 68B — 3 pkts

5 of 5 ‹ 1 ›

Event details

	Field	Value
☑	@timestamp	[redacted] @ 00:27:29.802
□	_id	ioTY-nYBLJMagDUQ9CXf
□	_index	auditbeat-7.9.0-2020.12.15-000001
□	_score	1

Enable Security Analytics Across Your Attack Surface

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

ABOUT ELASTIC

Elastic makes data usable in real time and at scale for enterprise search, observability, and security. Elastic solutions are built on a single free and open technology stack that can be deployed anywhere to instantly find actionable insights from any type of data — from finding documents, to monitoring infrastructure, to hunting for threats. Thousands of organizations worldwide, including Cisco, Goldman Sachs, Microsoft, The Mayo Clinic, NASA, The New York Times, Wikipedia, and Verizon, use Elastic to power mission-critical systems.