neosec

Neosec ShadowHunt

Managed Threat Hunting Service for APIs

ShadowHunt

Neosec ShadowHunt is a managed threat hunting service that enhances your security team with expert Neosec analysts skilled in API threat hunting. Ideal for understaffed teams or those lacking API security expertise, Neosec ShadowHunt is an outsourced resource that helps you reduce risk. Neosec threat hunters work as an extension of your team to detect and report on the most clandestine and obfuscated attacks hiding in your API traffic.

Neosec API Security Platform Plus Human Expertise

The Neosec API security platform offers comprehensive API Security features including:

API discovery:
Broad and continuous API discovery

Risk posture:
Understand your API risks

Threat detection using behavioral analytics:
Our big data, cloud based analytics engine examines all API activity over time continually detecting API abuse

Prevention and response:
Customized, conditional response playbooks enhance security and API DevSeOps processes

Investigation and threat hunting:
Powerful investigation capabilities that provide the ability to hunt for threats hiding in your API traffic

Key Benefits

- Peace of mind that experts are examining your API activity
- Detect more security threats lurking in your API data
- More time for your team while Neosec focuses on API security
- Actionable insights for software development & IT operations
- Improved visibility into API behavior

Threat hunting is one of the most advanced capabilities of the Neosec API security platform. The Neosec ShadowHunt service is intended for customers that lack either the tools, expertise, or time to threat-hunt.

How Managed Threat Hunting Works

ShadowHunt operations begin with the API activity data in the Neosec cloud platform. These automated analytics detect behavioral deviations and vulnerability exploits. Machine learning signals are then delivered to ShadowHunt analysts for investigation. This is where human expertise begins. Since analysts are familiar with customer API estates, they will rapidly identify active threats and create and transmit a ShadowHunt Alert. If there is ambiguity in the findings, an analyst will contact a ShadowHunt subscriber for clarification.

Analysts and the Neosec API security research team consume threat intelligence information in order to deliver periodic emerging threat reports to all service customers.

ShadowHunt Services You Can Rely On

ShadowHunt

ShadowHunt Alerts

Immediate notification of a threat in your API estate. The most important element of the Neosec ShadowHunt service is the Alert, transmitted immediately upon confirmation of an active incident.

Alerts include:

- Incident findings and analysis
- Threat Intelligence summary pertaining to incident
- Remediation recommendations

ShadowHunt Threat Report

Gain early API security intelligence. The ShadowHunt Emerging Threat Report is based on the team's access to global threat intelligence, input from the Neosec API security research team and ongoing threat hunting activities.

The Emerging Threat Report includes:

- Details of new API vulnerabilities, threat or attack identified by the team
- Impact on your API estate
- Remediation recommendations as needed.

ShadowHunt Monthly Review

Full visibility into your API estate. The ShadowHunt Monthly Threat Report is delivered to all Neosec customers in the first week of each month.

It includes:

- Summary of ShadowHunt Alerts and Emerging Threat Reports sent in the previous month
- API estate overview
- API activity comparison from the past two months
- Security headlines from the API industry.

ShadowHunt Ask the Experts

Service subscribers have access to the ShadowHunt team for questions and discussions about both Alerts and Emerging Threat Reports.

Threat hunting expertise to protect your APIs

The explosive growth in API deployments can place strains on organization IT security departments. The Neosec ShadowHunt Service enhances your security staff today.

Why Neosec?

Neosec is reinventing API security by applying the principles of Extended Detection and Response (XDR) to the challenge of securing APIs from vulnerabilities and API abuse. Only Neosec aggregates API activity into its cloud-based big data environment, followed by complex data enrichment and organization. This unique architecture enables continuous API discovery, risk scoring, context-aware behavioral analytics to detect API abuse and threats, and threat hunting. The Neosec architecture includes privacy by design, wherein any API activity destined for the Neosec cloud can be tokenized.

Reinventing API Security
Request product trial at Neosec.com

Gartner COOL VENDOR 2022

RSAC Innovation Sandbox 2022 FINALIST

neosec