Radware Threat Intelligence Service

In today's complex digital landscape, security operations center (SOC) engineers face numerous challenges. They frequently encounter blocked IP addresses lacking clear context and suspicious sources that keep their teams on edge. Additionally, network teams require real-time visibility and the capability to proactively defend against threats before they escalate. Data-driven decision-making is crucial. Radware Threat Intelligence Service directly addresses these challenges, offering invaluable insights and solutions.

Key Features

Actionable Data from Real Cyberattacks

Leverage Radware's cyberattack data and intelligence to gain actionable insights. All data originates from production environments, capturing real attacks launched by active threat actors.

Futureproofed Business Continuity

The Reputation Alert service identifies compromised systems and proactively notifies organizations of potential cyberattacks originating from within their own network.

Empowered SOCs That Make Informed Decisions

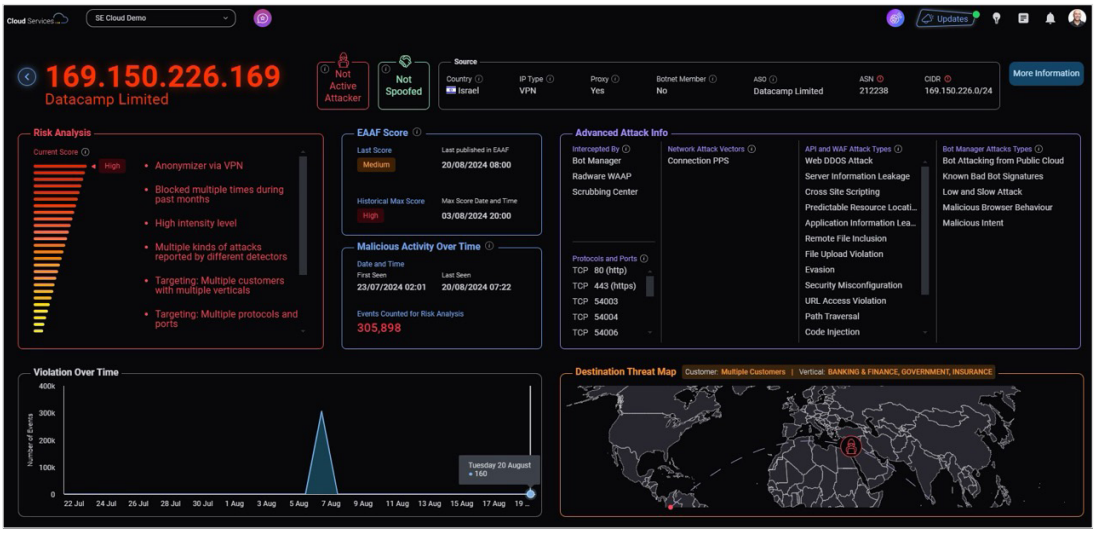
Enhance the quality and depth of data in the SOC/SIEM system for more thorough analysis of security events. You'll empower security teams to make more informed decisions, leading to improved threat detection and response and lower MTTR.

Seamless Integration With Any Environment

The service homepage is just a click away in the Radware Security Cloud Portal. It can also be fully integrated into existing security workflows via a REST API.

Figure 1

Unified insights screen providing visibility into enriched data collected by Radware



Inside Radware Threat Intelligence Service

Research Any Suspicious IP Address

Radware Threat Intelligence Service features a search window that lets users investigate suspicious IP addresses and determine their legitimacy. The research results rely on large, diverse data sets to correlate the real-life data gathered from diverse sources in real-time. They are delivered through the following actionable information:

IP Insights

Gain visibility into cyberattack threat data collected in real-time from multiple interceptors. Raw data is transformed into comprehensive insights, including IP addresses involved in DDoS (web and network), WAF, API and bot attacks blocked by Radware.

Open Proxies and Malware Data

Enhance the context of source IPs by integrating external data feeds and Open-Source Intelligence (OSINT) with Radware's contextual insights for each IP.

Reputation Alert: Futureproof Continuity of Business

To avoid compromising the integrity and reputation of the organization, the Reputation Alert informs the organization of potential cyberattacks originating from their own network. Reputation Alert filters millions of events per day and correlates the relevant IP addresses to the organization into twice-a-day email alerts for predefined email contacts. Organizations that receive this alert should suspect:

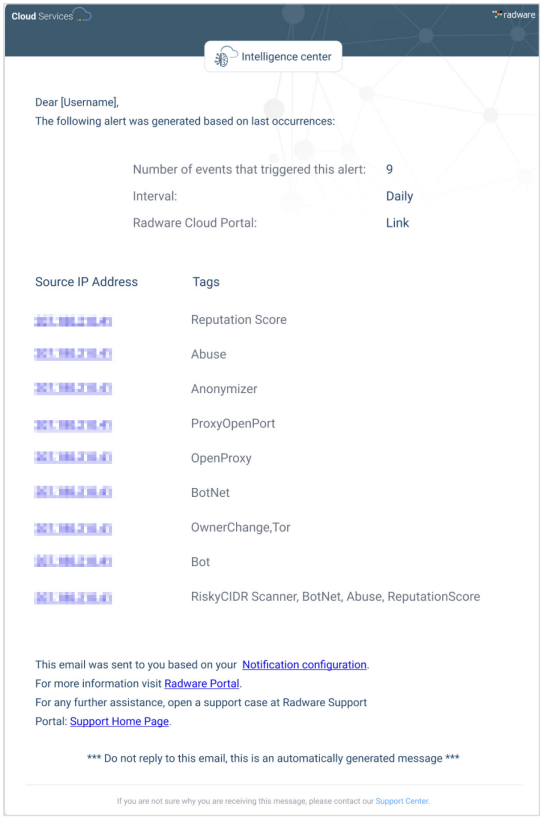
- The system has been compromised
- Assets have been associated with malicious or undesirable activity
- A vulnerable service is running on the network

The alert leverages data reported by one of Radware Interceptors or by observing the organization IPs with the OSINT interceptors.

By issuing preemptive warnings before outbound traffic blocks occur, Radware allows organizations to swiftly take action and prevent any disruptions, thereby assuring business continuity.

Figure 2

The Reputation Alert's notice informing organization of potential cyberattack originating from their own network



Empower SOCs to Make Informed Decisions

The service enhances the quality of data integrated into the SOC/SIEM system, transforming raw and real-time data into enriched, contextual information. This allows for more comprehensive analysis, enabling security teams to identify patterns and anomalies that might otherwise go unnoticed.

By providing enriched data from real-time production environments, SOC teams can enhance their threat detection capabilities, resulting in quicker identification and response to potential threats. This process ensures that the SOC can make precise and timely decisions, ultimately improving the organization's overall security posture, reducing the risk of breaches and lowering MTTR.

Fully Integrate With Existing Security Workflows and Systems

With just a click from the Radware Security Cloud Portal, teams can access the Radware Threat Intelligence Service homepage to research any suspicious IP addresses. To ensure seamless integration with existing security workflows and systems, our service is fully compatible with the Threat Intelligence REST API. This API provides quick and comprehensive access to critical data, enabling security teams to efficiently incorporate real-time threat intelligence into their operations. By leveraging this integration, organizations can enhance their security measures and respond to threats more effectively.

Figure 3

Example for a Threat Intelligence REST API call

```
curl --location --request POST
'https://api.radwarecloud.app/api/v1/sdcc/threat/core/insight/_bulkResolve' \
--header 'x-api-key: {{x-api-key}}' \
--header 'Context: {{Context}}' \
--data-raw '{
    "addresses": ["8.8.8.8", "8.8.4.4"],
    "projection": ["all"]
}'
```

Find Your Threat Intelligence Service Plan

Consider which plan is right for your organization: The Free plan, which is open to all Radware Cloud customers, supports current subscription and portal activity. The Essential and Pro plans offer advanced capabilities and extended scale of the service and are available for purchase to all customers.

Figure 4

At-a-glance look at Radware Threat Intelligence Service plans

Plans	Free	Essential	Pro
IP Insight			
Monthly IP Queries	50	300,000	1,000,000
Who IS - AS, Geo and Range	✓	✓	✓
Risk Score and AI Analysis	✓	✓	✓
Intelligence - Malware, Proxy, Active Attackers and Bot Net	✓	✓	✓
REST API Support	✗	✓	✓
Reputation Alert			
Monitored Subnets Beta	✗	5	10
Intelligence			
Telegram Claimed Attack Reports	✗	✗	Future

Transform Uncertainty into Clarity

Radware Threat Intelligence Service unravels the mystery behind specific actions, shedding light on why certain IPs were flagged and enabling informed decisions. While the services dive deep into these sources, distinguishing between legitimate and potentially malicious activity, actionable intelligence will allow you to confidently assess threats. Armed with this knowledge, you can proactively defend against threats before they escalate. Whether it is blocking a suspicious IP or fine-tuning your defenses, we have you covered.

By leveraging Radware Threat Intelligence Service you will transform uncertainty into clarity, bolstering your organization's security posture. Welcome to a new era of threat intelligence.

RWI 339 I 11.26.2024