SAFEDASH

CYBER ANALYTICS

SafeDash I About US

At **Safedash**, we are committed to empowering businesses with the tools and resources they need to navigate the ever-changing landscape of cyber threats confidently.

Our mission is clear - to simplify your security journey by providing cutting-edge testing tools and easy access to valuable data, allowing you to focus on what matters most: your business's growth and success.

SafeDash I About US

Our core values reflect our commitment to excellence, innovation, and customer-centricity. We believe in:

Security First: Security is our top priority, and we take proactive steps to find and fix any weaknesses or vulnerabilities. We are fully committed to making sure our testing tools are as secure as possible in all aspects of our work.

Customer Success: Our success lies in the success of our customers. We are committed to understanding their unique needs and challenges, providing personalized solutions that align with their goals.

Continuous Innovation: The cyber threat landscape is ever evolving, and so are we. We embrace innovation and stay ahead of the curve, constantly refining our tools and services to address emerging threats.

Collaboration and Partnership: We view our clients as partners in their security journey. Collaboration is at the heart of our approach, as we work together to achieve shared objectives.

Empowering Security Knowledge: We believe that knowledge is power. Alongside our services, we are dedicated to educating our clients about the latest security trends and best practices.

SafeDash | Product Portfolio

CAST DDoS

- Cloud based solution.
- Easy to setup BOTNET.
- White-listed DDoS attack traffic all the way to end customer from 11 regions.
- Real time and post reports.
- Do it by your self. (optional)

CAST LOAD

- Protocol based, functional based & customized LOAD tests.
- Cloud based solution.
- Easy to setup BOTNET.
- Real time and post reports.
- Do it by your self. (optional)

CAST DDoS

CastDDoS | Security as Process

- All successful businesses evolve over time, and their IT has to change with it. Simultaneously the tools and techniques attackers and criminals use to try and exploit businesses change as well.

- One of the critical part of the process is testing. If a company invests in some kind of defense measure e.g. DDoS protection and then does not test it, it could be spending money on a capability which does “nothing” and thus does not fulfil the requirements of the business case. This is as true for DDoS mitigation as it is for systems that prevent penetration and data theft.

- Suffice to say that DDoS testing is a critical part of being secure and being seen to be secure.

CastDDoS I Why invest in DDoS Testing?

DDoS testing is crucial to proactively uncover and address vulnerabilities in your company's defence system. A successful DDoS testing aims to uncover the following aspect of your company's cybersecurity posture:

- **Resilience Against DDoS Attacks:** DDoS testing evaluates the resilience of an organization's network and infrastructure against DDoS attacks, which aim to overwhelm systems with a flood of traffic, making services unavailable to legitimate users.
- **Capacity Planning:** It helps in understanding the capacity limits of an organization's current infrastructure and can guide decisions on necessary upgrades or changes to withstand high volumes of traffic.
- **Mitigation Strategy Evaluation:** Organizations can test the effectiveness of their DDoS mitigation strategies, including rate limiting, traffic shaping, and scrubbing services, ensuring that they can effectively filter out malicious traffic without impacting legitimate users.
- **Incident Response Planning:** Through DDoS testing, organizations can develop and refine incident response plans to quickly and efficiently respond to DDoS attacks, minimizing downtime and service disruption.

CastDDoS I Why periodic DDoS testing is important?

A DDoS attack may target DNS servers, application servers, routers, firewalls and internet bandwidth. The need for periodic DDoS testing depends heavily on how much your business relies on e-commerce, online sites & applications. If your organization must maintain 24/7 online presence, this type of security assessment is essential.

Regularly testing DDoS defenses provides the following essential safeguards against having DDoS protection go stale:

- Verifies that end-to-end connectivity continues to work as expected.
- Validates the operational run books applied to your service:
- Makes you focus on what you need to defend.

CastDDoS I Why CastLOAD?

Cloud based:

2000+ Nodes and up to 700 gbps traffic

Comprehensive:

150+ Pre-Defined Tests

Geographically diverse:

White-listed DDoS attack traffic all the way to end customer from 11 regions

Agile:

System designed to be scaled up or down very quickly

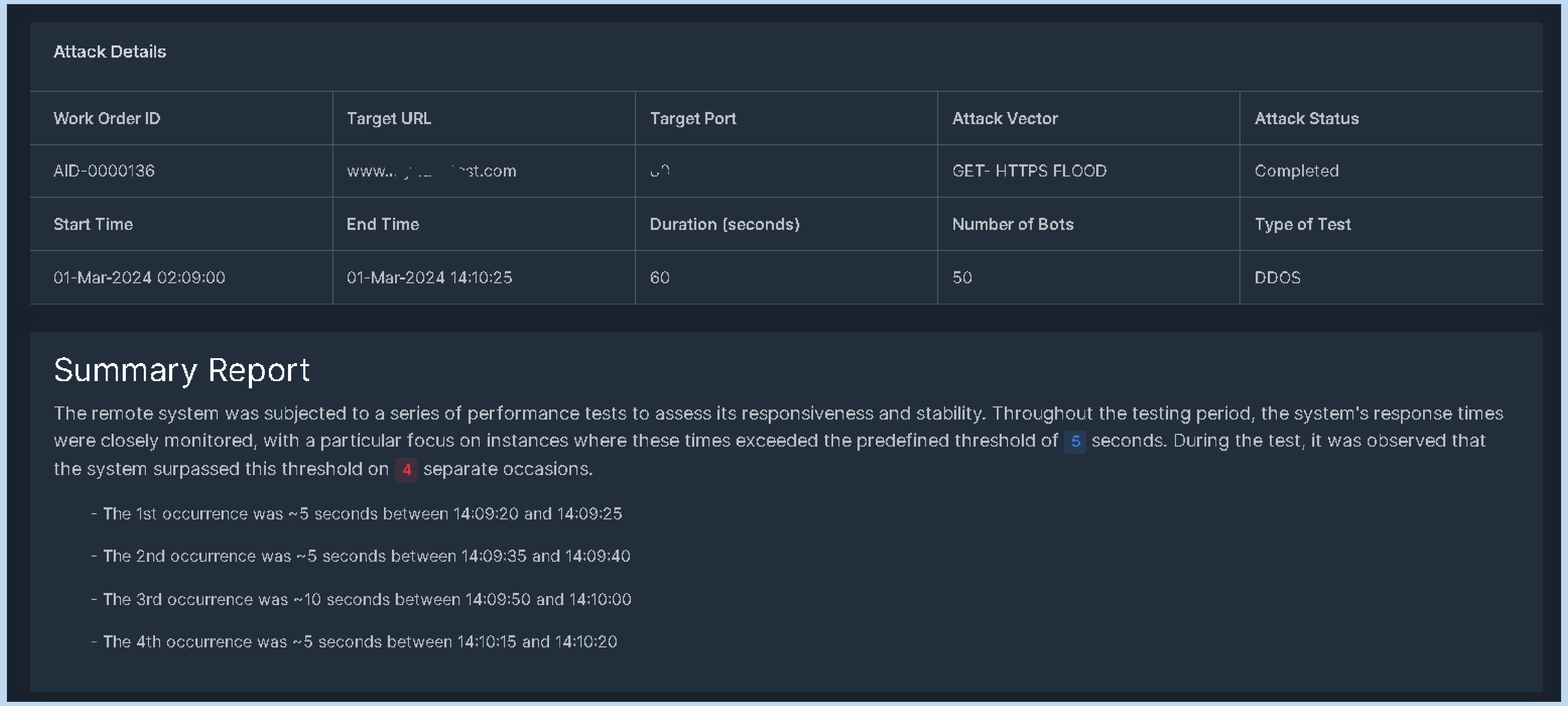
Bespoke:

All attack types and scripts developed in-house by CAST DDoS and can be modified very easily according to customer requests

User friendly:

Very easy to start the attack on one click and get report immediately.

CastDDoS I Screen Samples-01



Attack Details

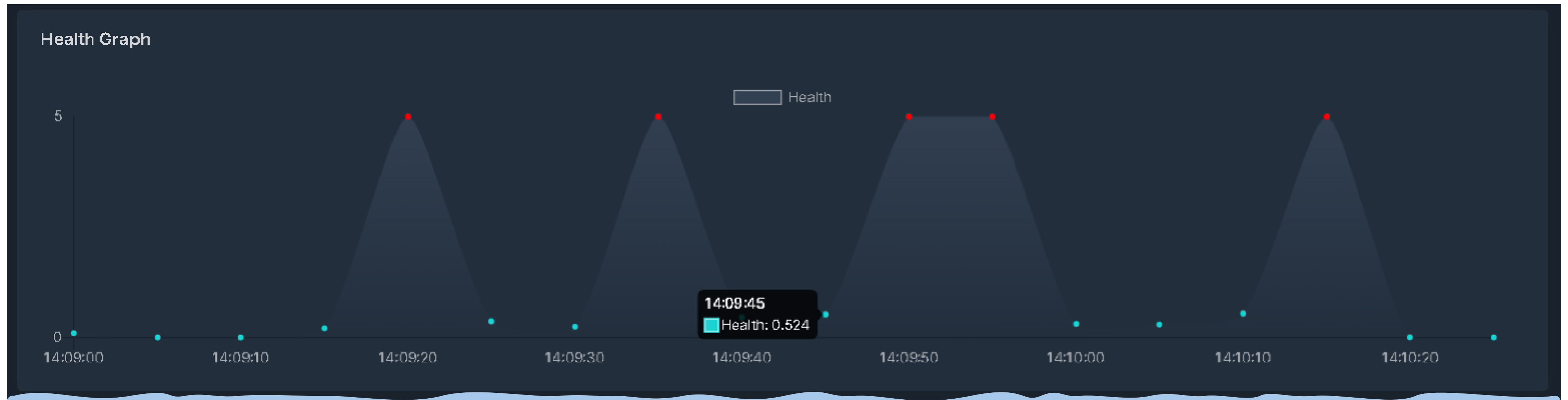
Work Order ID	Target URL	Target Port	Attack Vector	Attack Status
AID-0000136	www.[redacted]st.com	[redacted]	GET- HTTPS FLOOD	Completed
Start Time	**End Time**	**Duration (seconds)**	**Number of Bots**	**Type of Test**
01-Mar-2024 02:09:00	01-Mar-2024 14:10:25	60	50	DDOS

Summary Report

The remote system was subjected to a series of performance tests to assess its responsiveness and stability. Throughout the testing period, the system's response times were closely monitored, with a particular focus on instances where these times exceeded the predefined threshold of 5 seconds. During the test, it was observed that the system surpassed this threshold on 4 separate occasions.

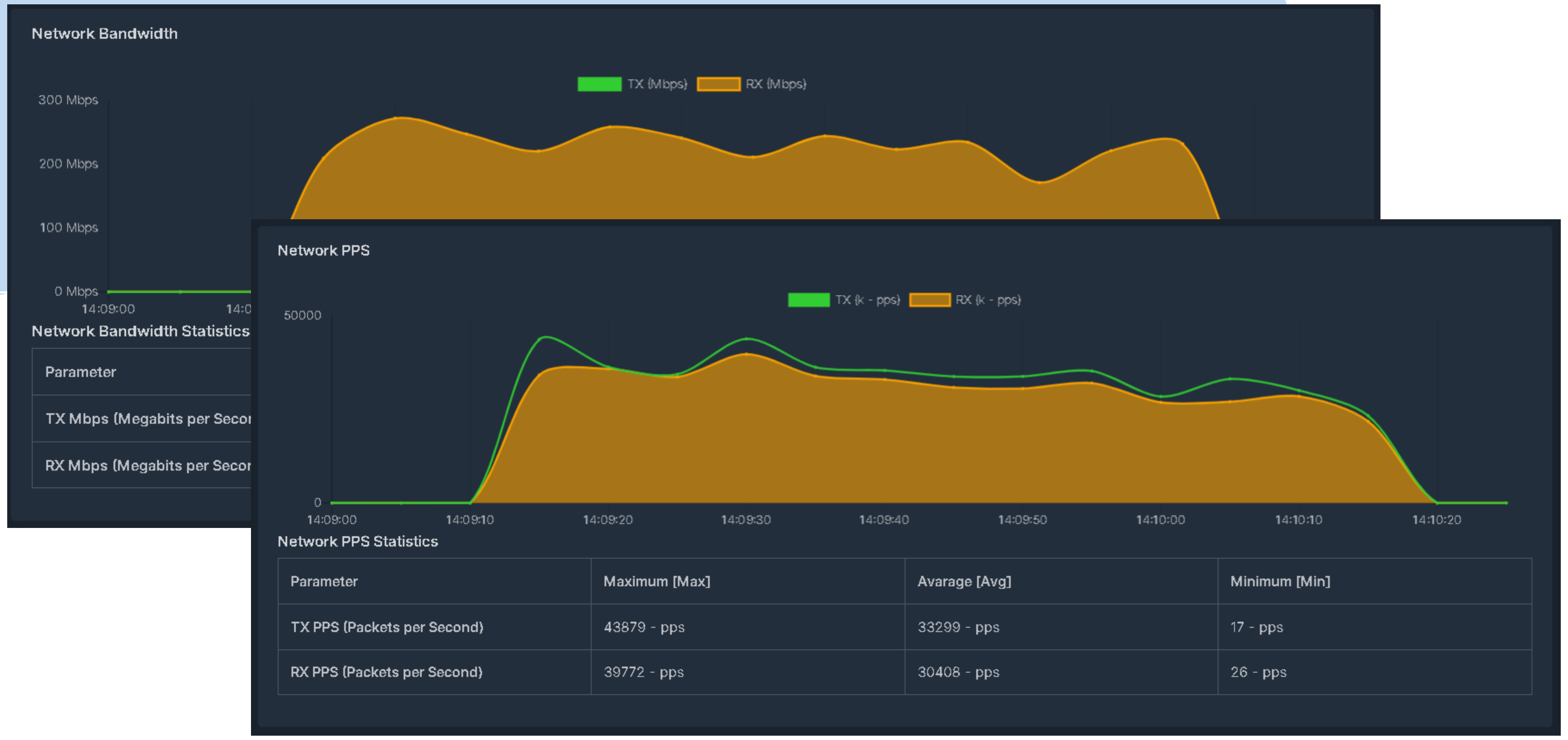
- The 1st occurrence was ~5 seconds between 14:09:20 and 14:09:25
- The 2nd occurrence was ~5 seconds between 14:09:35 and 14:09:40
- The 3rd occurrence was ~10 seconds between 14:09:50 and 14:10:00
- The 4th occurrence was ~5 seconds between 14:10:15 and 14:10:20

The report gives you key details about the attack like the website URL targeted, the port used, the kind of attack, when it started and ended, how long it lasted, how much time it was actively running, and the type of test conducted. Additionally, the system automatically creates a summary report. This summary includes important information and how the targeted system reacted, including moments when the system went down, which the system detects and handles automatically.



Health Graph

The report displays key details about whether the target system is working properly, using graphs that change over time. This information, along with data about network activity measured in packets per second (pps) and bytes per second (bps), is really helpful. It helps us figure out how much the system can handle and how it responds to the test traffic



Network Bandwidth

Network Bandwidth Statistics

Parameter
TX Mbps (Megabits per Secor
RX Mbps (Megabits per Secor

Network PPS

Network PPS Statistics

Parameter	Maximum [Max]	Avarage [Avg]	Minimum [Min]
TX PPS (Packets per Second)	43879 - pps	33299 - pps	17 - pps
RX PPS (Packets per Second)	39772 - pps	30408 - pps	26 - pps

The report shows important information about the attack through graphs over time and specific numbers. It includes the maximum, average, and minimum amounts of data sent (Tx) and received (Rx) both in packets per second and bytes per second.

CAST LOAD

CastLOAD I Why invest in Load/Stress Testing?

Investing in load and stress testing is an investment in your product's quality, user experience, and reliability. CastLOAD helps identify how well the application can handle a large number of concurrent users and transactions and can help pinpoint any performance bottlenecks or issues that may arise under heavy loads. It enables proactive problem-solving, ensures efficient resource use, and supports a seamless growth strategy.

- **Performance Issues:** Highlighting how load testers can detect problems like slow response times, high latency, or server crashes when multiple users access the application simultaneously.
- **Scalability:** Demonstrating the ability of load testers to evaluate an application's capacity to scale and handle increased user loads over time. This is crucial for understanding how well an application can grow to meet demand without degradation in performance.
- **Capacity Planning:** Assisting organizations in determining the necessary infrastructure and resources needed to support their application under expected loads. This is essential for efficient resource allocation and ensuring a smooth user experience.
- **Security Vulnerabilities:** Showing that load testing can also uncover potential security risks under heavy load conditions. Identifying such vulnerabilities is critical for preventing attacks that could exploit these weaknesses, like denial of service (DoS) attacks.

CastLOAD I Why CastLOAD?

In today's online world, the strength and reliability of your platform are crucial. Here's what makes CastLOAD a top choice:

- **Ease of Use:** Let us worry about the complicated stuff. You focus on what the results mean for your business.
- **Flexibility:** Our system can quickly adjust to your growing needs, making it easier to expand whenever you need to.
- **Worldwide Testing:** Perform tests from over 50 locations across the globe, ensuring your platform can handle users from anywhere.
- **Clear Results:** Get straightforward access to how your platform is performing, with all the complex data simplified for you.
- **Smart Insights:** With real-time analytics, you have the power to make informed decisions on how to improve your platform continually.

This approach ensures CastLOAD not only meets but exceeds your expectations by providing a robust, user-friendly, and insightful load testing experience.

CastLOAD I 3 Different Product Types

Protocol Based Load Test

- HTTP/HTTPS
- SOAP
- WEB API
- WEB SOCKET

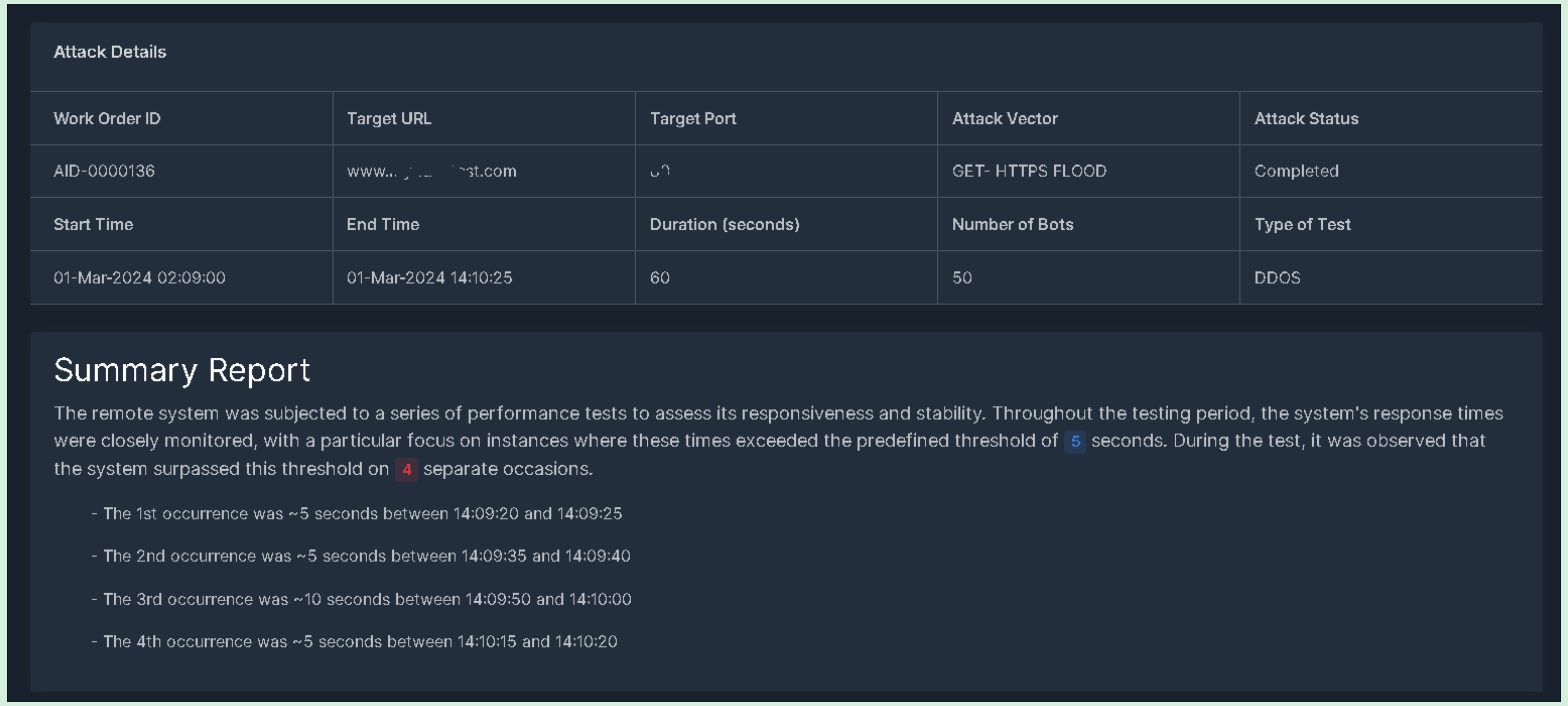
Functional Based Load Test

- Selenium
- APACHE JMeter™
- POSTMAN

Media Streaming Test

- HTTP live streaming

CastLOAD I Screen Samples-01



Attack Details

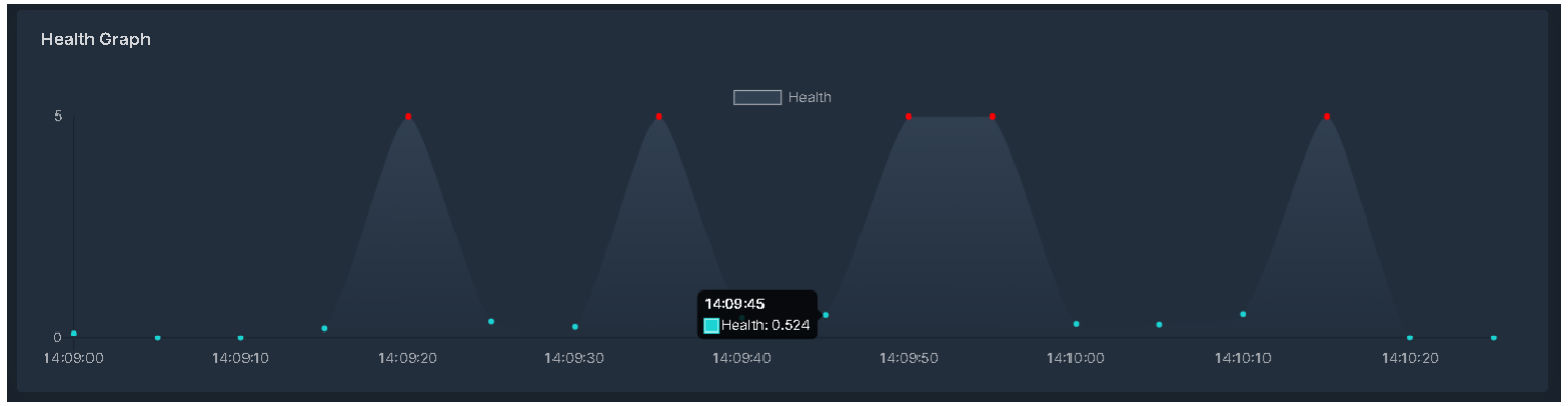
Work Order ID	Target URL	Target Port	Attack Vector	Attack Status
AID-0000136	www.[redacted]st.com	[redacted]	GET- HTTPS FLOOD	Completed
Start Time	**End Time**	**Duration (seconds)**	**Number of Bots**	**Type of Test**
01-Mar-2024 02:09:00	01-Mar-2024 14:10:25	60	50	DDOS

Summary Report

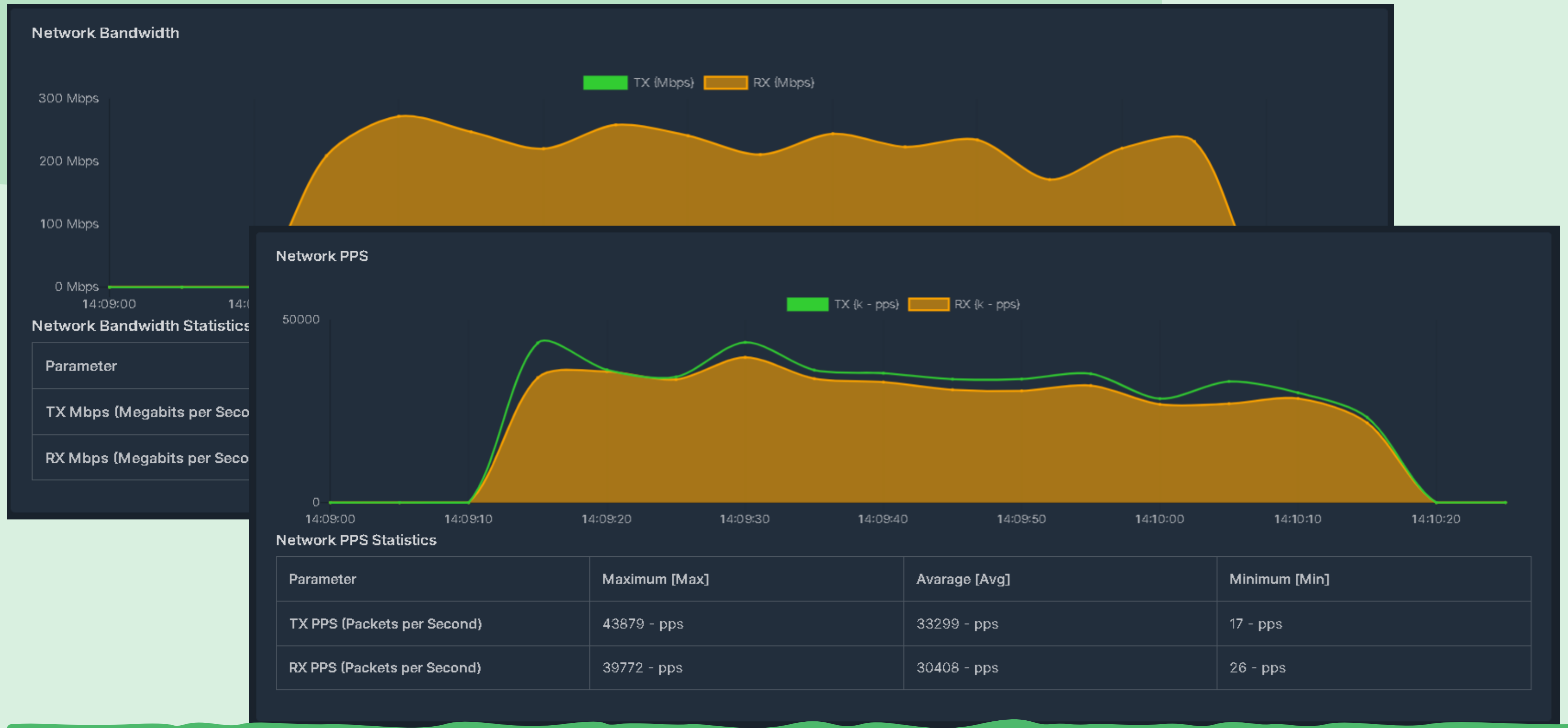
The remote system was subjected to a series of performance tests to assess its responsiveness and stability. Throughout the testing period, the system's response times were closely monitored, with a particular focus on instances where these times exceeded the predefined threshold of 5 seconds. During the test, it was observed that the system surpassed this threshold on 4 separate occasions.

- The 1st occurrence was ~5 seconds between 14:09:20 and 14:09:25
- The 2nd occurrence was ~5 seconds between 14:09:35 and 14:09:40
- The 3rd occurrence was ~10 seconds between 14:09:50 and 14:10:00
- The 4th occurrence was ~5 seconds between 14:10:15 and 14:10:20

The report gives you key details about the attack like the website URL targeted, the port used, the kind of attack, when it started and ended, how long it lasted, how much time it was actively running, and the type of test conducted. Additionally, the system automatically creates a summary report. This summary includes important information and how the targeted system reacted, including moments when the system went down, which the system detects and handles automatically.



The report displays key details about whether the target system is working properly, using graphs that change over time. This information, along with data about network activity measured in packets per second (pps) and bytes per second (bps), is really helpful. It helps us figure out how much the system can handle and how it responds to the test traffic



Network Bandwidth Statistics

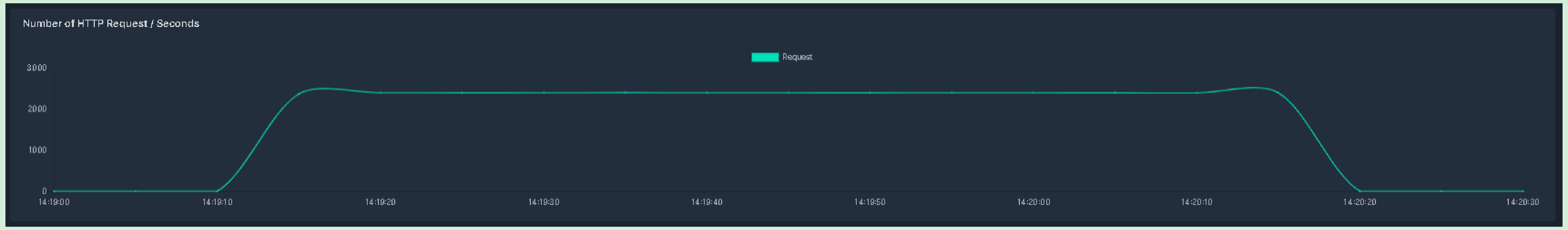
Parameter
TX Mbps (Megabits per Seco
RX Mbps (Megabits per Seco

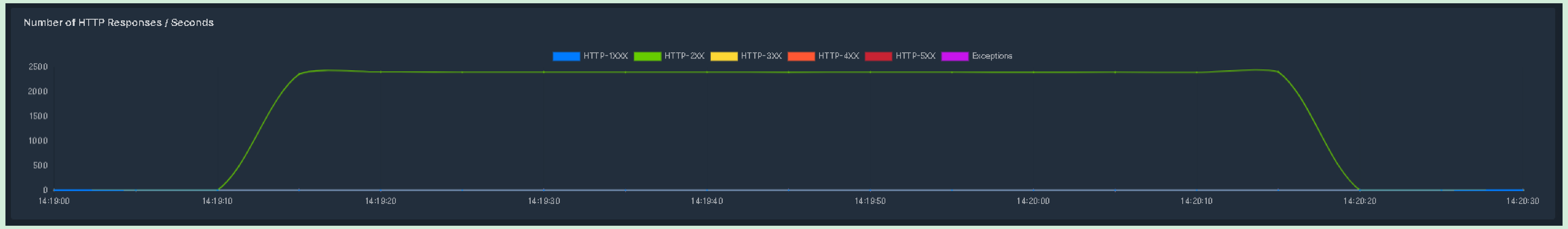
Network PPS Statistics

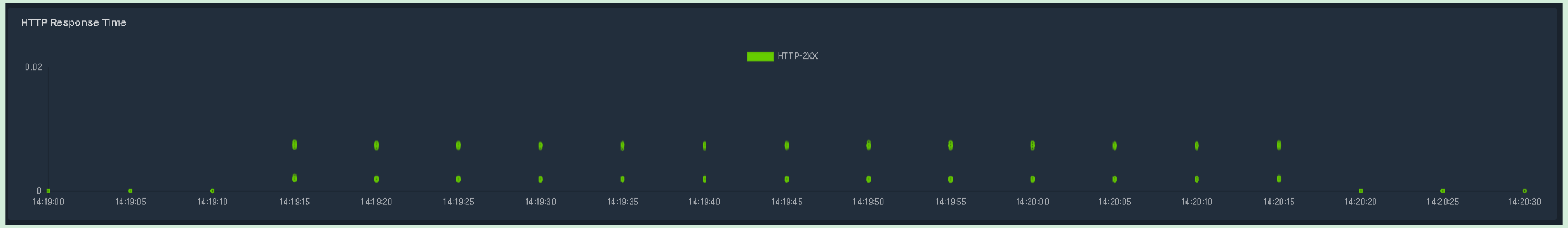
Parameter	Maximum [Max]	Avarage [Avg]	Minimum [Min]
TX PPS (Packets per Second)	43879 - pps	33299 - pps	17 - pps
RX PPS (Packets per Second)	39772 - pps	30408 - pps	26 - pps

The report shows important information about the attack through graphs over time and specific numbers. It includes the maximum, average, and minimum amounts of data sent (Tx) and received (Rx) both in packets per second and bytes per second.

CastLOAD I Screen Samples-01

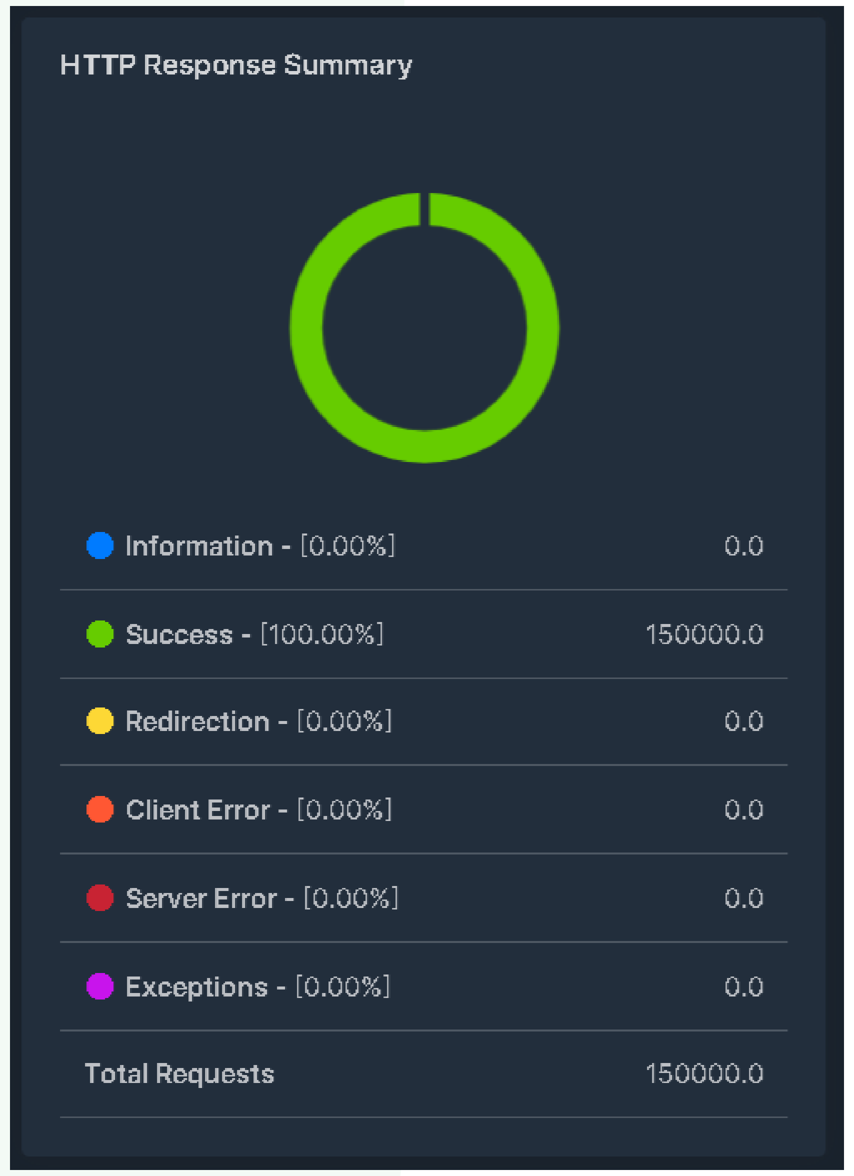






The report displays key details about HTTP Requests/second, response/second, response time (median) using graphs that change over.

HTTP Requests per Second: This measures the number of HTTP requests that your application can handle in one second. A high number indicates good performance and the ability to serve many users simultaneously. It's essential for understanding the application's scalability and identifying if and when it might need additional resources to maintain performance. Responses per Second: Similar to HTTP requests per second, this metric shows how many responses are successfully returned to users within a second. It helps gauge the efficiency of your server in processing and responding to incoming requests, which is directly related to user experience. A higher rate means that your application is quick to respond to user actions, which is critical for keeping users engaged and satisfied. Median Response Time: This metric offers a snapshot of how long it takes for your application to respond to requests, with a focus on the median value to avoid skewing by outliers. It's a reliable indicator of the responsiveness of your application under normal conditions. Shorter response times are indicative of a better user experience, as users expect quick reactions to their actions on modern web applications.



HTTP Response Summary

🟦 Information - [0.00%]	0.0
🟩 Success - [100.00%]	150000.0
🟨 Redirection - [0.00%]	0.0
🟧 Client Error - [0.00%]	0.0
🟥 Server Error - [0.00%]	0.0
🟪 Exceptions - [0.00%]	0.0
Total Requests	150000.0

The report shows important information about the attack through graphs over time and specific numbers. It includes the maximum, average, and minimum amounts of data sent (Tx) and received (Rx) both in packets per second and bytes per second.

In essence, these summaries offer a condensed, at-a-glance view of key performance indicators, enabling stakeholders to make quick, data-driven decisions to maintain and enhance the application's performance and reliability.

REFERENCES

YOROI®
TINEXTA CYBER

BORSA İSTANBUL

BIM

NETSYS

amazon

A10

TAKAS İSTANBUL

Turkey's Government Projects

BAUHAUS®

nebula
Trusted Security Advisor

HALKBANK

SAFEDASH

CYBER ANALYTICS

Thank You...