Email #1:
Email length: 58 words
Subject lines:

- DDoS Testing That's Always On, Never Down. (43 characters)
- The Critical Challenge DDoS Mitigation Vendors Have (50 characters)
- **Every mitigation vendor has this challenge…. (45 characters)**

Commented [1]: the best one
Commented [2R1]: Lets do it!

Hi {{first_name}},

If your organization operates online, it's vulnerable to DDoS risk.
The only way to eliminate DDoS vulnerabilities is to be constantly testing for them.

That's why [redacted] developed [redacted] testing. It solves the critical challenge that every DDoS mitigation vendor has.

This video explains that challenge:
[redacted]

Email #2: SENT IF NO REPLY
Email length: 61 words
Subject lines:

- Get the Most Accurate DDoS Testing Standard (43 characters)
- ***We need a game-changing standard in DDoS testing (42 characters)***
- I want to tell you exciting news about DDoS testing (56 characters)

Hi {{first_name}},

There is some exciting news you need to know.

Commented [3]: Note: Take this out if you decide on subject line #3.

[redacted] uncovered a new standard for DDoS testing after constantly running anti-DDoS tests for other companies.

Unlike other types of DDoS testing, [redacted] testing is always-on and never down, constantly testing for vulnerabilities in your network so you can eliminate them.

Do you have 5 minutes this week so I can show you?

Please find a relevant asset

Email #3: SENT IF NO REPLY
Email length: (59 words)
Subject lines:

- DDoS Testing that is DDoS-Mitigation Agnostic?! (48 characters)
- **Overcome Your DDoS Vulnerability Gap. Here's how. (49 characters)**

A certain percentage of vulnerabilities succeed in bypassing a company's DDoS mitigation vendor –the *vulnerability gap*.

Every mitigation vendor has this challenge.

[redacted]testing works with any DDoS mitigation vendor to solve the critical challenge that every vendor faces.

Interested? I can show it to you in action in a 5-minute call this week.
Link to meeting

Email #4: SENT IF NO REPLY
Email length: (57 words)
Subject lines:

- I can show you the vulnerabilities in your system [NAME] (56 characters)
- Let's take a look at all the vulnerabilities in your network [NAME] (66 characters)
- ***Want DDoS testing more than just 2 times a year [NAME]? (40 characters)***
- Get DDoS testing that's more than just 4 times a year [NAME] (62 characters)

Commented [4]: the best IMO

And that's if you're lucky

I can promise you that there are many vulnerabilities hidden in your network.

With [redacted]testing, you'll get continuous DDoS testing all year long, so you're constantly on the lookout for vulnerabilities.

Let me show you how in a short demo. Do you have time for a quick chat this week?

vi
Also, have a look at our CEO and Founder [redacted]talking about the challenge
[redacted]

Email #5: SENT IF NO REPLY
Email length: (57 words)
Subject lines:

- **Huge brands are still going down after a DDoS attack. Why? (58 characters)**
- Overcome Your DDoS Vulnerability Gap. Here's how. (50 characters)

Commented [5]: used almost this already.... try not to repeat?

Commented [6]: used almost this already.... try not to repeat?

I can bet you that they had the best DDoS mitigation systems in place too.

Unfortunately, even the best DDoS mitigation systems are unable to constantly test and eliminate vulnerabilities in your network.

Those vulnerabilities that slip through – the "vulnerability gap" – are a critical challenge for every DDoS mitigation system.

Always-on and never down, [redacted] testing eliminates the vulnerability gap.
Read about it here:

Add assets related to the vulnerability gap
https://blog.[redacted]/eliminate-ddos-vulnerability-gap

Email #6: LAST ONE IN CADENCE
Email length: (94 words)
Subject lines:

- Don't miss the most accurate standard in DDoS testing [NAME] (52+characters)
- **There is another way to approach DDoS testing [NAME] (53 characters)**

Commented [7]: used almost this already.... try not to repeat?

I haven't gotten a reply from you yet.

But I want to make sure you understand that there's a new accurate standard out there for DDoS testing.

Always-on and never down, [redacted] testing is the only solution that constantly tests every attack vector against every target without disruption.

Plus, it's DDoS mitigation agnostic, so it works with whatever system you already have in place.

If I don't hear from you, I'll assume you're not interested in having the new standard of DDoS testing ….

But if you are… When would you have time for a quick demo so I can show you?

Link to meeting