Which of these attack types is the most prevalent threat to your organization?

+ Over 2 in 5 respondents (43%) say Distributed Denial of Service (DDoS) attacks are the most prevalent threat to their organization
+ A third of respondents (33%) say ransomware attacks are the most prevalent threat to their organization
+ Just under 1 in 5 respondents (19%) say zero-day malware attacks are the most prevalent threat to their organization
+ 1 in 16 respondents (6%) say no attack type is most prevalent to their organization

Have you experienced a DDoS attack in the past 24 months?

+ Over 4 in 5 respondents (83%) say they have experienced a DDoS attack in the past 2 years, with over half (51%) saying they’ve experienced an attack several times
+ 1 in 6 respondents (16%) say they haven’t experienced a DDoS attack in the past 2 years, with over half (51%) saying they’ve experienced an attack several times
QUESTION 3:
If yes, how many hours of downtime did your organization experience from the DDoS attack?

+ On average, respondents who have experienced a DDoS attack within the past 2 years, say they experienced 12 hours of downtime due to an attack.

+ Over half of respondents who have experienced a DDoS attack within the past 2 years (52%), say they have experienced 5-10 hours of downtime due to an attack, with 3 in 10 experiencing 11-20 hours (30%).

+ 1 in 12 respondents who have experienced a DDoS attack within the past 2 years (8%), say they have experienced 21-30 hours of downtime due to an attack.

QUESTION 4:
What would you consider as the most dire consequence to companies caused by a DDoS attack?

+ More than a third (36%) of respondents consider the most dire consequence caused by DDoS attacks is revenue loss.

+ Just over a third (34%) of respondents consider decreased IT staff productivity as the most dire consequence for companies caused by DDoS attacks.

+ 1 in 5 (20%) of respondents think that reputation damage is the most dire consequence for companies caused by DDoS attacks.

QUESTION 5:
Do you have a DDoS protection provider or tool?

+ 1 in 9 respondents (11%) don’t have a DDoS protection provider or tool, whilst 1 in 16 (6%) are not sure.

+ Over 4 in 5 respondents (83%) have a DDoS protection provider or tool.
Have you experienced a cyberattack on any of your web applications in the past 24 months?

+ Over 4 in 5 respondents (81%) have experienced a cyberattack on their web applications in the past 2 years, with nearly half experiencing a cyberattack several times (46%)

+ Just over 1 in 6 respondents (17%) haven’t experienced a cyberattack on their web applications in the past 2 years

How would you rate your website and application security performance?

+ 1 in 11 respondents (9%) say their website and application security performance is unsatisfactory

+ Just over 9 in 10 respondents (91%) say their website and application security performance is satisfactory, with nearly 3 in 5 (57%) saying it’s highly satisfactory

If you did experience a cyberattack to one of your web applications, how much did it cost your company?

+ On average, respondents in the U.S. said the most recent cyberattack cost their company USD $152,439.10
QUESTION 9:
Which cybersecurity technologies do you use managed service providers for?

+ Almost three quarters of respondents (73%) use managed service providers for cloud-based firewalls
+ Just over 7 in 10 respondents (71%) use managed service providers for DDoS protection
+ Over 3 in 5 respondents (62%) use managed service providers for email security

QUESTION 10:
Do you scan and test for vulnerabilities on web applications?

+ Over 9 in 10 respondents who have web applications (97%) say they scan and test for vulnerabilities within their web applications, with just over two thirds (67%) saying they always scan and test for vulnerabilities