Summary of findings

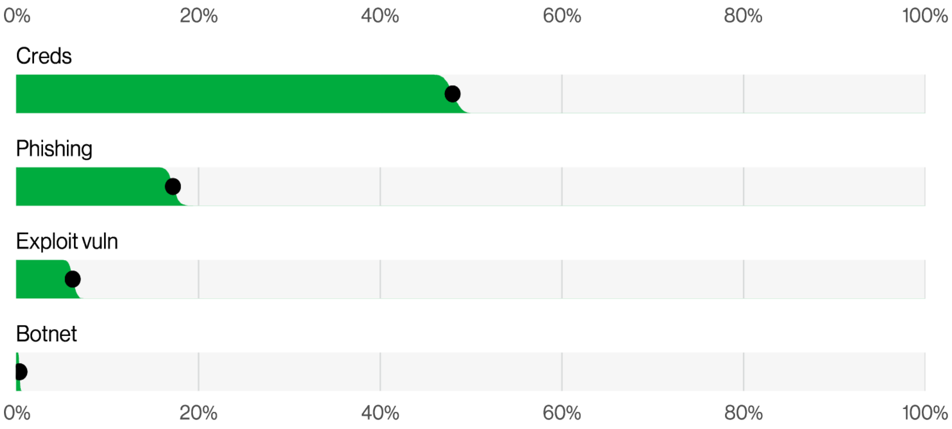

Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

There are four key paths leading to your estate: Credentials, Phishing, Exploiting vulnerabilities and Botnets. These four pervade all areas of the DBIR, and no organization is safe without a plan to handle them all.

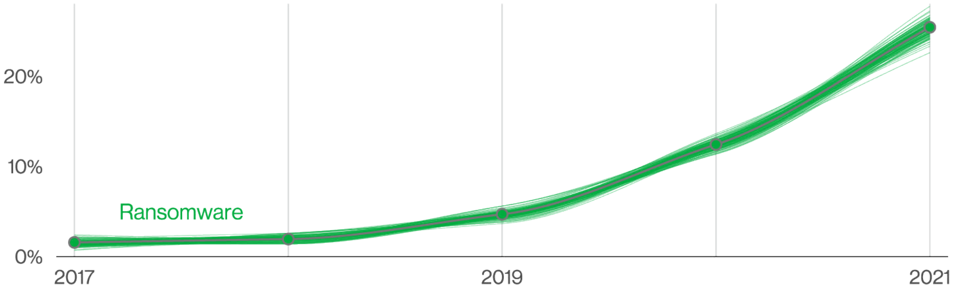

Figure 6. Ransomware over time in breaches

This year, Ransomware has continued its upward trend with an almost 13% increase–a rise as big as the last five years combined (for a total of 25% this year). It's important to remember, Ransomware by itself is really just a model of monetizing an organization's access. Blocking the four key paths mentioned above helps to block the most common routes Ransomware uses to invade your network.

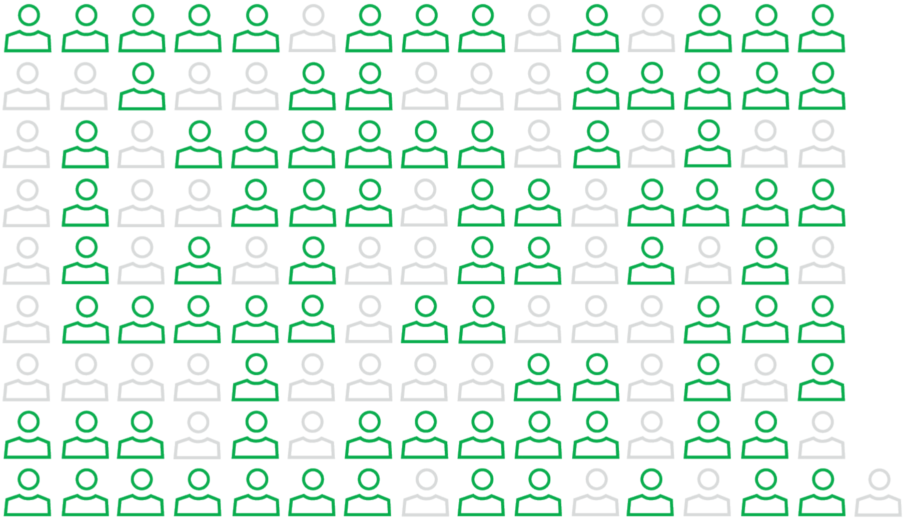

Figure 7. Partner vector in System Intrusion incidents (n=3,403)
Each glyph represents 25 incidents.

2021 illustrated how one key supply chain breach can lead to wide ranging consequences. Supply chain was responsible for 62% of System Intrusion incidents this year. Unlike a Financially motivated actor, Nation-state threat actors may skip the breach and keep the access.

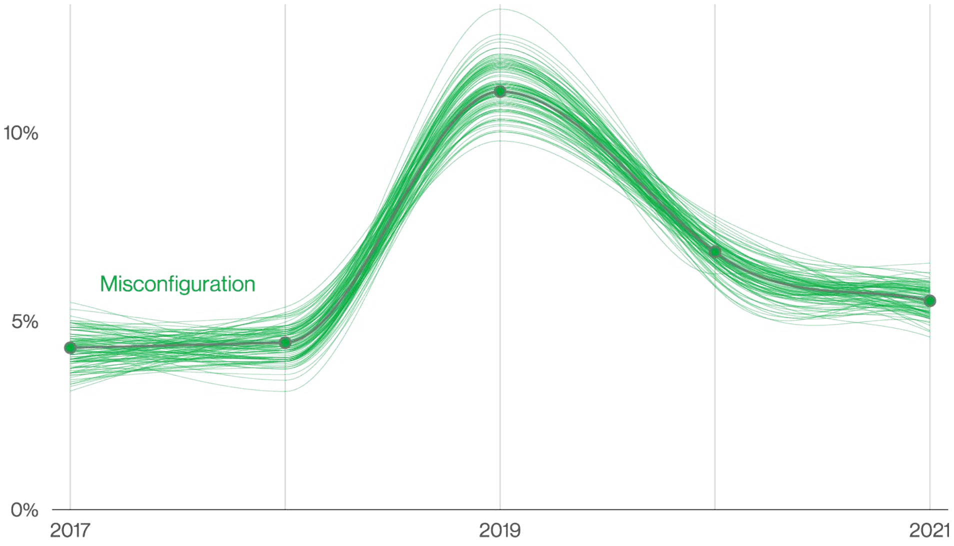

Figure 8. Misconfiguration over time in breaches

Error continues to be a dominant trend and is responsible for 13% of breaches. This finding is heavily influenced by misconfigured cloud storage. While this is the second year in a row that we have seen a slight leveling out for this pattern, the fallibility of employees should not be discounted.

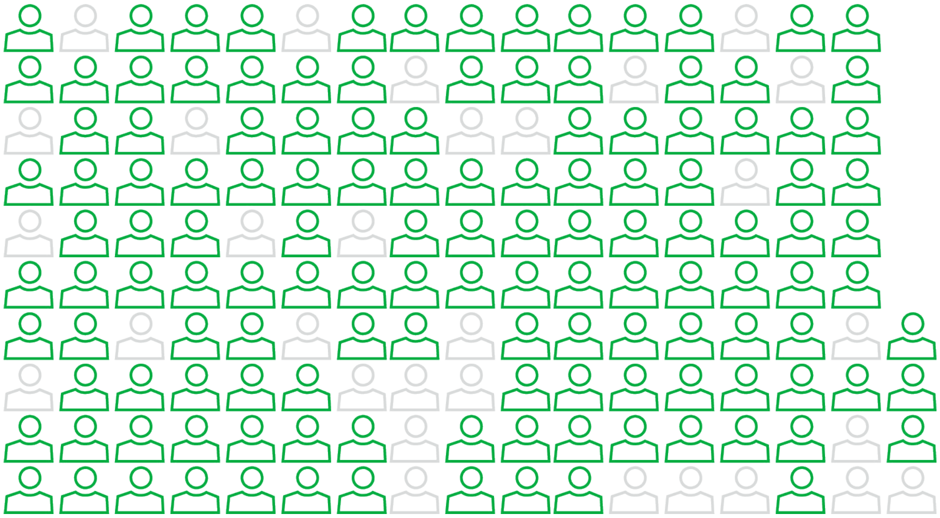

Figure 9. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

The human element continues to drive breaches. This year 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing, Misuse, or simply an Error, people continue to play a very large role in incidents and breaches alike.