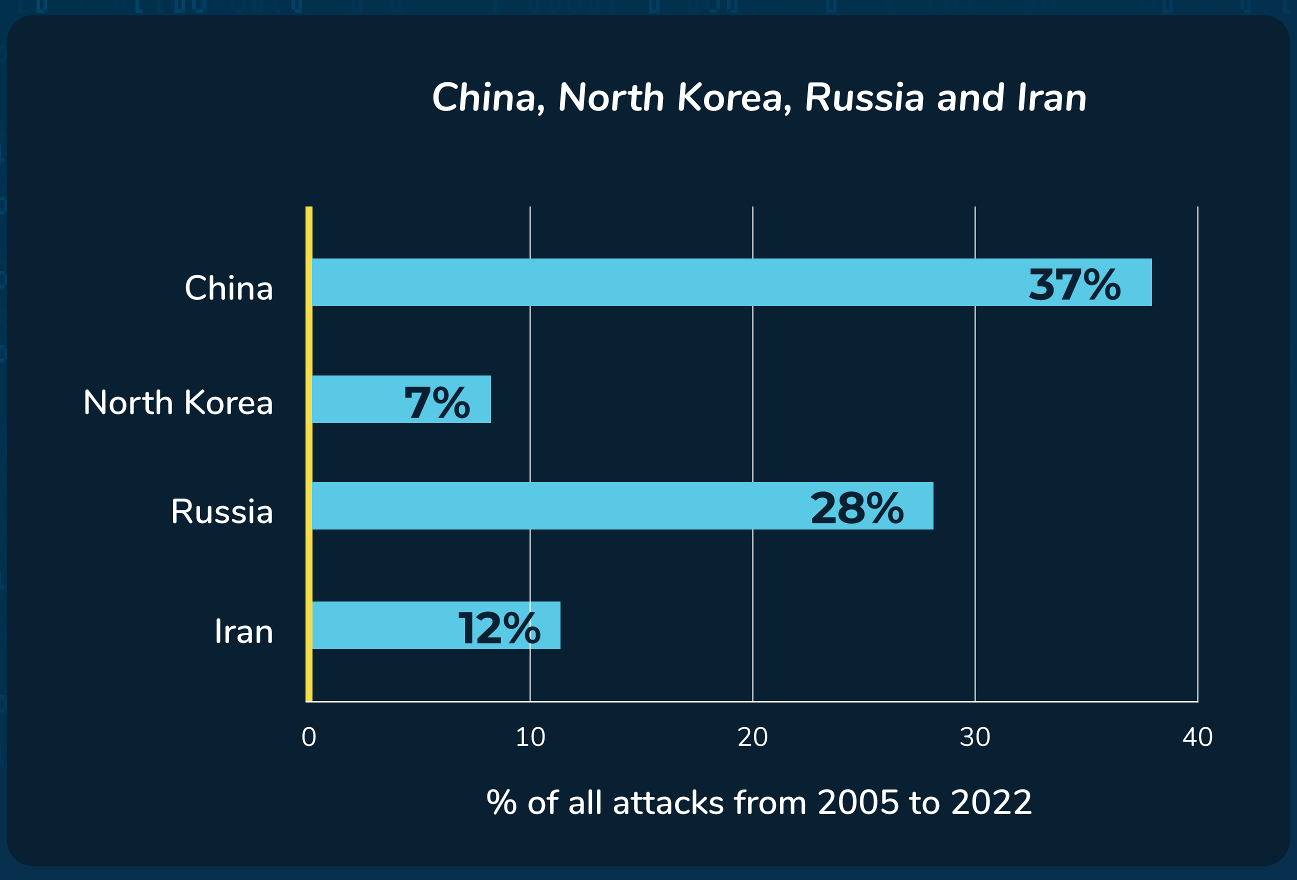
THE NEW (CYBER) ADMINISTRATION

The Department of Defense (DoD) and other federal agencies are working to protect mission-critical assets from advanced persistent threats (APTs). As agencies contend with these savvy nation-state and non-state actors, policymakers are releasing guidance on how agencies can improve investigative efforts.

With this in mind, what does the current threat landscape look like? And how will new policies help government organizations build a more robust security posture?

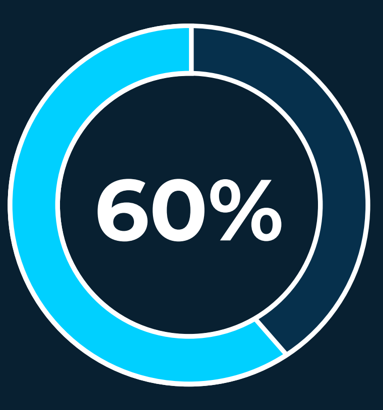
CYBERTHREATS AT A GLIMPSE



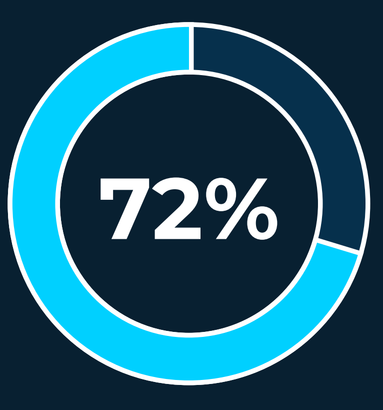
77% of all intrusions can be traced back to three initial access vectors:

- Phishing
- Software Vulnerabilities
- Brute-force Credential Attacks

CONFIDENCE AMID A CHALLENGING LANDSCAPE



60% of federal, defense and local leaders feel “somewhat confident” in their ability to respond to cyber threats



72% feel as if their agency is moving in the right direction as it pertains to cybersecurity policies and procedures

POLICY CHANGES ACROSS THE FEDERAL GOVERNMENT

What’s new?

Policy releases like OMB Memorandum 21-31 (M-21-31) are changing how federal civilian and DoD leaders approach investigative efforts. M-21-31 supports greater incident response outcomes in three key ways by:

- Establishing basic logging categories
- Defining minimum logging data requirements
- Mandating centralized access to all event logging data

AI, M-21-31 AND YOU

One of the unspoken benefits of M-21-31 is that it sets the stage for agencies to effectively leverage contemporary technologies like artificial intelligence and machine learning (AL/ML). With AI/ML government organizations can effectively address common vulnerabilities and enhance incident response times.

For example, with Cortex XSIAM, an intelligent platform, one organization was able to reduce its mean time to resolution down to **just 16 minutes**.

AI/ML also helps agencies:

- Reduce costs associated with data ingest
- Proactively outpace threats via automated continuous discovery

LEARN MORE & EXPLORE

But that’s just the tip of the iceberg. To learn more about the intersection of AI/ML and M-21-31, visit Presidio Federal’s Palo Alto Partnership Site.

PRESIDIO® FEDERAL paloalto® NETWORKS immixGroup An Arrow Company