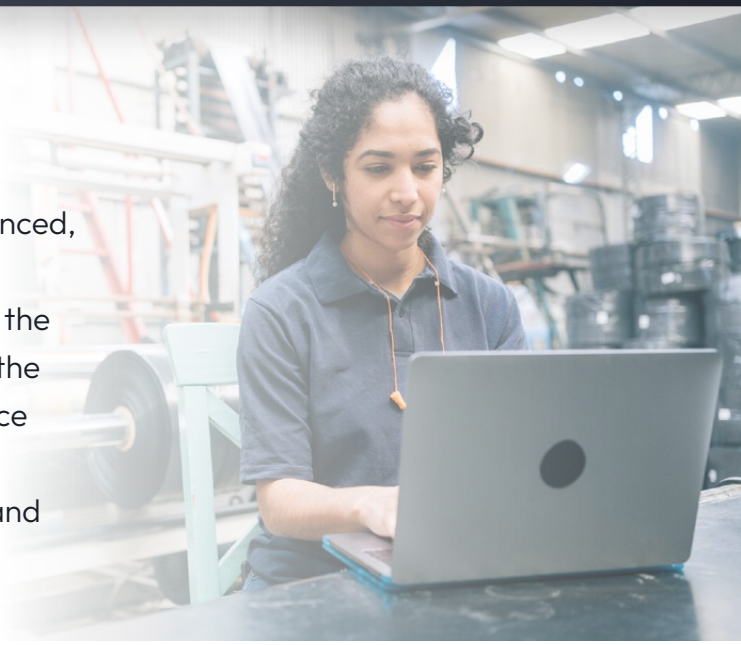
DomainTools

Case Study

DomainTools helps investigate advanced persistent threats and protect brand for global aerospace and defense company



Business Challenge

As one of the largest global aerospace and defense contractors, this Fortune 500 company provides advanced, mission-critical systems and services for commercial, military, and government customers worldwide. Given the highly-sensitive nature of the company's industry and the irreplicable value of their intellectual property, they face multifaceted cybersecurity challenges across multiple business lines from highly sophisticated threat actors and state-sponsored cyber espionage efforts.

Global aerospace and defense company

Customer Profile

Leading aerospace and defense contractor

Business Objective

Brand monitoring; proactive defense and response to Advanced Persistent Threats (APTs)

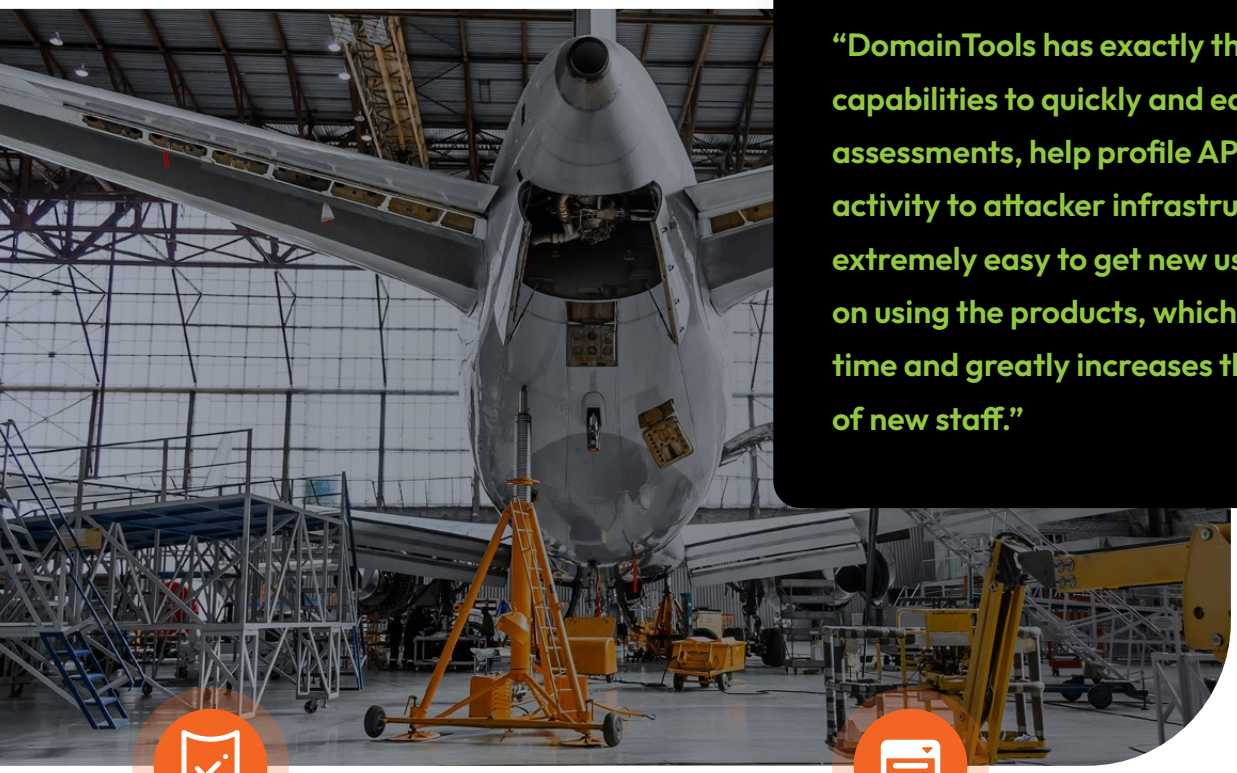
DomainTools Solution

Iris Investigation Platform

Business Outcomes

Real-time monitoring of domain-based threats and historically enriched indicators of threat infrastructure

The company maintains a mature cybersecurity organization of over 500 members that operate with world-class cybersecurity capabilities. Even so, staying ahead of cyber threat actors whose own capabilities are increasing in sophistication is no easy feat.



"DomainTools has exactly the right mixture of capabilities to quickly and easily perform risk assessments, help profile APTs, and map cyber activity to attacker infrastructure. Plus, it's extremely easy to get new users up to speed on using the products, which saves us a lot of time and greatly increases the work efficiency of new staff."

DomainTools is the global leader for internet intelligence and the first place security practitioners go when they need to know. The world's most advanced security teams use our solutions to identify external risks, investigate threats, and proactively protect their organizations in a constantly evolving threat landscape.

The ability to enrich indicators of compromise (IoCs) has also become more complicated as data protection and privacy laws have limited the visibility of data traditionally used for identifying, assessing, and sharing information on potential threats and known attack infrastructure. This makes comprehensive data sources and access to extensive passive DNS records critical to track the evolution of threat actor campaigns via the domains and IP addresses they have previously used.

Approach

Focused on staying ahead of advanced persistent threat (APT) groups and state-sponsored actors, the security organization utilizes the DomainTools Iris Investigation Platform collaboratively across several primary teams including the Operations Group, incident response, threat intelligence, threat hunting, and threat assessment teams.

The defense contractor's Director of Cyber Threat Intelligence said that DomainTools gives the teams a comprehensive infrastructure intelligence platform to research suspicious activity and provides his team with high-quality indicator enrichments when it comes to contextualizing attack infrastructure, especially for domains, nameservers, and other DNS infrastructure that they can quickly translate into actionable threat intelligence.

The extensive historical archive DomainTools provides is a major asset for the cyber threat intelligence (CTI) team, allowing them to make connections and pivot to understanding the infrastructure a known actor influences, controls, or is actively weaponizing. "Historical data is especially useful for putting together connections that we would have previously missed, especially when we may have lost some visibility due to data collection restrictions," said the Director of Cyber Threat Intelligence. DomainTools solutions are built on an unmatched 15 years of data, which include Whois records, passive DNS data, related screenshots, IP addresses, hosting data, name servers, and other DNS data.

The customer has come to depend on DomainTools to protect its brand online by leveraging its unique visibility into over 315 million current domains and 200,000 domain observations per second. This enables brand monitoring alerts that signal when a threat actor is in the beginning stages of registering domains—for a phishing campaign or other malicious activity—even before they're provisioned in DNS. A keyword search allows the team to investigate and build detections and blocklists that expand beyond just the domain name. By seeing the larger infrastructure surrounding a domain name, they're able to anticipate a threat actor's next move and preemptively monitor or block domains that at first seem unrelated.

Results

The customer utilizes insights provided by DomainTools to better understand the networks and infrastructure of state-sponsored actors and other highly-motivated parties looking to compromise their network.

Knowing whether the adversary they are up against is well organized and in control of their own capabilities allows the company to move quickly beyond a reactive "monitor and response" strategy and mobilize a proactive defensive posture to triage threats and prevent attacks before they happen.

DomainTools has become a critical component of the company's brand protection process and strengthens their overall proactive security posture. "We are able to know, in real-time, when a potentially malicious, or even slightly suspicious, domain is registered and act on it immediately," said the Director of Cyber Threat Intelligence "Oftentimes before it even has the chance to get used."

About DomainTools

DomainTools is the global leader for internet intelligence and the first place security practitioners go when they need to know. The world's most advanced security teams use our solutions to identify external risks, investigate threats, and proactively protect their organizations in a constantly evolving threat landscape.