DomainTools

Case Study

The Business Value of Proactive Threat Intellience with DomainTools

IDC research confirms the value for customers leveraging DomainTools enterprise security solutions data to identify and address potential threats. DomainTools customers interviewed by IDC reported minimizing their risk exposure while greatly enhancing the capabilities and efficiency of their threat investigation teams.

Key Results

$784,700

Value in higher productivity per year, threat investigation teams

313%

Average 3 year ROI

5 months

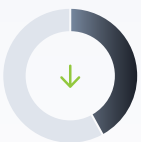
To payback

CUSTOMER QUOTE

"We have faster incident response and better visibility into threat intelligence with DomainTools, which enhances our overall business efficiency."

Improved Threat Intelligence Capabilities

82% faster
to identify threats



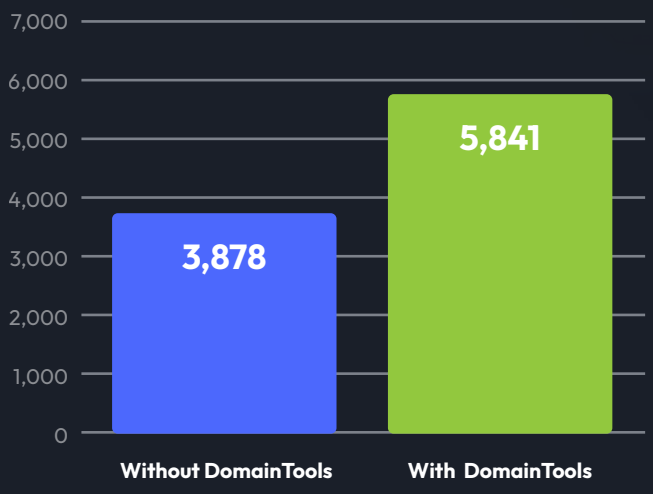
42% fewer
events

Nearly 3x more
threats identified

19% lower
chance of incidents

Threat Investigation Team Productivity Gains

Supported employees per security team FTE



51% Higher productivity

Less staff time to achieve same levels of security

- **34%** Overall threat investigation team
- **28%** Incident management teams
- **24%** Security analyst team
- **45%** Other threat investigation team members

Voice of DomainTools Customers

AVOIDING IMPACTFUL EVENTS

"With DomainTools, we're able to identify malicious activities sooner and respond to it before business or operational risk occurs and prevent the impact connected with asecurity incident"

DELIVERING PROACTIVE INTELLIGENCE

"The most significant operational benefit of using DomainTools is being able to expose threat actor infrastructure and then taking that reactive information and turning it into proactive intelligence."

THREAT INTELLIGENCE EFFECTIVENESS

"DomainTools provides visibility into the actors that control the infrastructure that we're aware of and maps that to other infrastructure..... We can find out what other domains they control as well."

domaintools.com