IDC
ANALYZE THE FUTURE

Sponsored by:
DomainTools

Authors:
Christopher Kissel
Matthew Marden

June 2020

Business Value Highlights

313%
average three-year ROI

5 months
to payback

82%
faster to identify threats

Almost 3x
more threats proactively identified

42%
fewer events

19%
lower chance of incidents

51%
more productive threat investigation teams

The Business Value of Threat Intelligence with DomainTools

EXECUTIVE SUMMARY

There is an increasing chasm between the number of qualified cybersecurity professionals and the number of people needed to fill those roles. Security operation center (SOC) professionals often have to determine the potential outcomes of events with little contextual information at hands. DomainTools is a vendor that seeks to address these challenges by offering a context-rich cyberthreat intelligence solution. The company's approach involves using reputation scoring of domains to develop risk assessments, profile attackers, guide investigations, and map cyberactivity to attacker infrastructure.

IDC spoke with a number of large enterprises about their use of DomainTools security solutions to identify and respond to potential threats. According to the National Initiative for Cybersecurity Careers and Studies, an "event" is when there is an observable occurrence on a network or an information system. Events are what trigger an investigation in the first place, and events have a wide range of outcomes — an event can be a temporary network occurrence such as a bottleneck caused by latency or a security appliance generating a false positive. If an event cannot be accounted for as a benign instance, an event becomes an incident.

An incident happens when a vulnerability or an exploit to information/data on a network or system is a possible result. There are various ways to investigate the severity of an incident beginning with file integrity management or violations to firewall policies. However, an important forensic tactic used in the SOC is to monitor the ingress/egress activities of suspected devices for security-related anomalies such as malware hashes, visits to an untrusted website, or indications of C2C server activity.

It is within this context that organizations reported leveraging DomainTools to significantly improve their ability to perceive, understand, and link actor domains to potential threats, thereby reducing their operational risk and enabling their teams responsible for identifying and addressing threats to be much more productive. Overall, IDC quantified the average value that

IDC
ANALYZE THE FUTURE

interviewed DomainTools customers will realize as worth $830,100 per organization, which they will achieve by:

- **Significantly improving their capabilities for identifying and responding to potential threats** through proactive identification and resolution
- **Reducing operational risk** by having the visibility and information needed to take steps to eliminate potential threats and cut off actual security events before they more significantly impact business operations, including by:
  - **Detecting events proactively by determining domain risk scores:** If properly understood, a risk score can determine if a domain name system (DNS) request is forwarded to a potentially malicious domain. Preventing an event is the process of blocking a domain before a theft, breach, or device takeover occurs.
  - **Preventing incidents by understanding the forensic chain that produced the risk score and taking proper remedial actions:** An incident occurs when a network has been exploited. An exploit can be benign (relatively) like a print server has been pwned for a DDoS attack or extreme like records that have personally identifiable information (PII) have been exfiltrated. In other words, an incident is what happens when a breach has occurred.
- **Empowering a variety of network defense and threat investigation teams** to work with much greater effectiveness, thereby allowing those teams to cover more endpoints and devices with improved results
- **Optimizing security-related costs and supporting business activities** by delivering cost-effective but enhanced security environments that support agile and confident business activities

SITUATION OVERVIEW

The routing of the internet is powered by two concepts: the DNS and IP addresses. DNS is an application layer protocol used to associate authoritative DNS servers with the DNS database. DNS servers are the go-between for devices and subnets and the various domain name registrar services run by Internet Corporation for Assigned Names and Numbers (ICANN) and other organizations with similar functions. An IP address is no different than a street address and is expressed as either an IPv4 or IPv6. Memorizing IP addresses is problematic, and an additional naming convention is needed to associate the IP address with its location — **www.domaintools.com** for example. Internal to a mail server, the DNS function is used

extensively in internal networks to help identify assets in subnets and assign IP addresses. Finally, when devices connect to a DNS server, the DNS goes into a cache to begin the authentication process and to resolve whether a user is going to an allowed site or a blocked site.

Charting the origin and reputation of new IP addresses is problematic, and this dynamic figures to become more acute as microservices are erected and Internet of Things (IoT) come online. Naturally, the adversary will try to spoof brands or disguise command and control servers as functioning DNS servers.

However, cybersecurity professionals are not without recourse. Passive DNS monitoring can determine when a DNS server was activated online and what type of traffic is coming to and from the server. Self-evidently, newly spun up servers are more likely to be malicious than older ones, and traffic patterns that indicate beaconing have a different flow than ingress/egress traffic. Similarly, IP addresses can be cross-referenced with Whois to make sure that the IP address jibes with the registered website domain. (DomainTools has an extensive 18-year library of Whois names.)

A standard part of cybersecurity triage is to establish a timeline and investigate the machine or machines that have generated an alert and see where they have interacted with the internet. DomainTools establishes a risk score for each domain visited and enriches what is known about DNS requests emanating from devices to provide for better context in the investigation.

DOMAINTOOLS OVERVIEW

In the interview process, IDC asked survey participants which DomainTools products their organization was using. Specifically, IDC asked about four tools:

- **Iris Investigation Platform.** DomainTools Iris helps incident responders, threat hunters, and other SOC professionals understand the risk of internet domains and the infrastructure that supports them. Iris combines domain intelligence and predicted risk scoring with passive DNS data to guide threat investigations and uncover connected infrastructure.
- **Domain Risk Score.** The DomainTools Risk Score predicts the risk level and likely threats associated with a domain that has not yet been observed in malicious activities by analyzing intrinsic properties of the domain that are observable as soon as the domain is registered. The Domain Hotlist is a predictive and prioritized list of active, high-risk domains for proactive blocking, faster triaging, and more effective network monitoring.

- **PhishEye.** DomainTools PhishEye enables organizations to identify existing and new domains that spoof legitimate brands and products and carry out defensive or investigative actions against them. PhishEye is used to disrupt phishing campaigns such as business email compromise attacks and can block lookalike domains before the adversary uses them.
- **APIs.** DomainTools APIs are used to integrate DomainTools data into existing workflows and third-party tools for better threat resolution. One common example would be the DomainTools Enrich API used with Splunk to allow an investigator to see if a discovered malicious domain has been accessed by any end user.

Domain Risk Score was the most highly praised of these tools. In simple terms, security teams felt that triaging an alert by hand by mapping IP addresses to Whois registries, checking passive DNS logs for known associations with malicious sites using the DomainTools Proximity algorithm, and correlating activities from a DNS server with activities consistent with phishing or malware to come up with a risk score would be a laborious process and would likely produce a less accurate result than the machine learning–based DomainTools Risk Score based on huge volumes of aggregated DNS data.

THE BUSINESS VALUE OF DOMAINTOOLS ENTERPRISE SECURITY SOLUTIONS

Study Demographics

IDC conducted research that explored the value and benefits for organizations of using DomainTools solutions. The project included interviews with DomainTools customers with experience or knowledge about its benefits and costs. Interviews covered a variety of quantitative and qualitative questions about DomainTools' impact on their security and IT operations, businesses, and costs.

Table 1 presents study demographics and profiles. The organizations IDC interviewed had an average of 96,500 employees (median of 61,500), indicating an enterprise-level profile of study participants. This workforce was supported by an IT staff of 6,351 managing 2,094 business applications. The companies had data and storage capacity averaging over 5PB (5,630TB). In terms of geographical distribution, five companies were based in the United States, with one in Australia. There was a mix of vertical industries represented including the defense, financial services, government, manufacturing, oil and gas, and telecommunications sectors.

TABLE 1 Firmographics of Interviewed DomainTools Customers

	Average	Median
Number of employees	96,500	61,500
Number of IT staff	6,351	3,137
Number of business applications	2,094	900
Number of terabytes (TBs)	5,630	1,500
Revenue per year	$66.88 billion	$45.05 billion
Countries	United States (5), Australia	
Industries	Defense, financial services, government, manufacturing, oil and gas, and telecommunications	

n=6 Source: IDC, 2020

Choice and Use of DomainTools

Interviewed organizations described their use patterns and provided information about the environments secured and supported by the DomainTools platform. They also discussed the rationale behind their choice of the platform. Interviewed customers cited a number of factors including the solution's strong capabilities in mapping and linking threat actor infrastructure, the strong functionality of the DomainTools Iris platform, and user-friendly access to collected data. Study participants elaborated on these drivers of their choice of DomainTools:

- **Ability to collect and use threat intelligence data:** *"Ever since we started using DomainTools, their solutions have collected more information than anyone else and they have offered easy-to-use access to that data."*
- **Functionality of Iris and strength of DomainTools functionality:** *"I had experience using DomainTools in my previous position, and I pushed hard to use the Iris platform. Use of Iris is critical for investigations . . . We didn't really consider other solutions. DomainTools is the absolute leader in this space."*

Table 2 shows use by interviewed organizations of the DomainTools platform. Across study participants, DomainTools supported an average of 316 applications and 35 datacenters. Meanwhile, employees used an average of 163,333 devices on internal networks supported by DomainTools with a total average number of endpoints covered of more than 440,000 (see Table 2).

TABLE 2 Interviewed Organizations' Use of DomainTools

	Average	Median
Number of applications supported	316	70
Number of datacenters	35	10
Number of endpoints accessing internal networks	440,742	281,484
Number of employee devices accessing internal networks	163,333	90,000

n=6 Source: IDC, 2020

Quantifying the Business Value of DomainTools Enterprise Security Solutions

IDC's research confirms the value for study participants of using DomainTools enterprise security solutions to leverage data to identify and address potential threats. Interviewed DomainTools customers reported minimizing their risk exposure while greatly enhancing the capabilities and efficiencies of their threat investigation teams. They also discussed their much enhanced security-related capabilities and how these provided benefits from a risk and business operations perspective:

- **Avoiding risk through understanding malicious actors and preventing events:** *"Use of DomainTools is about risk avoidance. It's the ability for us to track the adversary, know what they are doing, understand what they are doing, and see how they are doing it. Basically, DomainTools allows us to collect threat intelligence, which is extremely valuable. It's also preventing and detecting the activity when it occurs. Situational awareness and prevention are huge for us."*
- **Improves capabilities for investigation and analysis:** *"We take information from our intelligence feed and enrich it as far as we can with DomainTools. Then we export that investigation and do additional transforms on the data. That interaction is valuable because we get more context, and the depth of the analyst's understanding is greater."*
- **More efficient business operations and reduced risk:** *"We have faster incident response and better visibility into threat intelligence with DomainTools, which enhances our business efficiency . . . Business units can be more efficient, and they can stop problems before they generate expenses. We have reduced disruptions, and whole business units have avoided incidents that affect one to two thousand people."*

Robust Threat Identification and Response

Today's enterprise security operations have several important fundamental requirements including enforcing existing security rules for firewalls, SIEM, and gateways; carrying out investigations when alerts indicate that these rules are being violated; and initiating mitigation and remediation steps when an alert is confirmed to be an actual security incident. Unfortunately, these processes tend to be reactive in nature. The DomainTools Investigation Platform and data sets are designed to help companies meet these challenges by adopting a more proactive approach to threat intelligence.

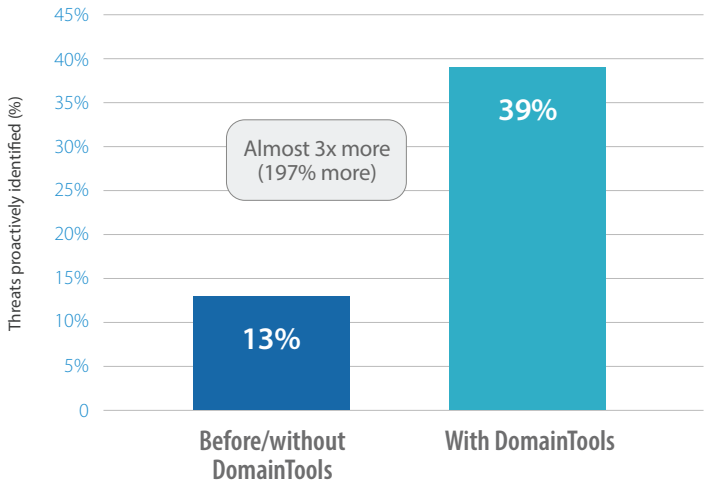
DomainTools uses key indicators from enterprise networks and data about threat actor infrastructure to arrive at robust threat identification and then develop attacker profiles, assess risk, and map cyberactivity to attacker infrastructure, thereby promoting situational awareness. Study participants spoke to IDC about how DomainTools provides access to significant amounts of data about potential bad actors as well as enhanced domain visibility into their actions. They also described how it enables the development of links between bad actors to provide a larger framework. In addition, they reported that DomainTools allows them to identify potential threats earlier and react more quickly and efficiently by initiating timely mitigation efforts. Study participants commented on these and other benefits:

- **Use of APIs to maintain current information about threats:** *"One of the big draws of DomainTools was using their APIs because we do a lot of automation on the cybersecurity side and can interact with their APIs to make requests directly to it in areas such as reputation and proximity scoring . . . Since DomainTools has current records, we can pull and update our own records to keep them up to date."*

- **Visibility into domain control enables proactive measures:** *"The most significant challenge that DomainTools helps with is providing visibility into the actors that control the infrastructure that we're aware of and mapping that to other infrastructure . . . Because we can now understand who controls a domain, we can find out what other domains they control as well."*

Better and more effective identification of threats is a key component of the DomainTools value proposition. As another study participant noted: *"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."* Figure 1 quantifies these benefits by looking at pre- and post-deployment data. As shown, the number of threats that interviewed organizations were able to proactively identify nearly tripled (197% increase) with DomainTools in place.

FIGURE 1 Identification of Potential Threats

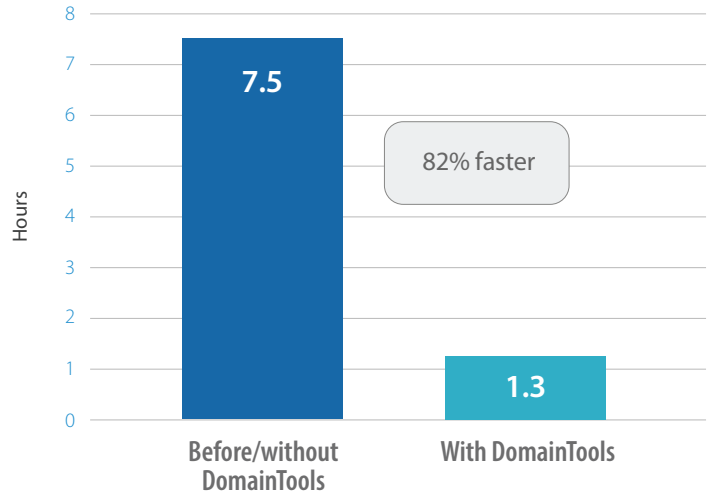


n=6
Source: IDC, 2020

Study participants reported that they can proactively identify more threats with the DomainTools platform in part because of the speed with which it feeds them actionable data. Likewise, faster access to robust data allows for more effective and timely mitigation steps. Addressing this capability, one study participant noted: *"We identify threats sooner with DomainTools because we have existing information. We identify them about 20% sooner."* Another noted: *"It took us 8–16 hours to identify a threat before deploying DomainTools compared with 5 minutes after deployment . . . With DomainTools, we're getting information that lets us be preventative and proactive. We're now identifying 35–40% of threats before they become impactful."*

Figure 2 quantifies this key benefit for study participants. As shown, the time required by organizations to identify threats has been reduced by 82%, representing a significant improvement over previous approaches taken. This has a significant practical impact for interviewed organizations; by speeding up their time to identify potential threats by an average of six hours, they can head off potential threats before they become impactful and more effectively mitigate the impact of events. Avoidance of potential threats and mitigation of actual security events both help DomainTools customers substantially minimize their overall risk profiles.

FIGURE 2 Time to Identify Potential Threats



n=6
Source: IDC, 2020

Reduced Operational Risk

As noted, study participants have leveraged the DomainTools platform to significantly reduce overall operational risk through proactive identification of and faster reaction to potential threats. IDC calculated that they have reduced the frequency of all events by an average of 42% and, as importantly, have lowered the risk of experiencing a major security breach or event by an average of 19%. One study participant noted: *"The threats we face are rapidly evolving, and DomainTools provides real-time data . . . The DNS tools are very useful, and we use pretty much the whole DomainTools platform to hunt threats. This allows us to map out and chart them and find convergences."*

Study participants cited a variety of ways in which use of DomainTools has helped lower risk including the advantage of having access to real-time data, preventing security events that could lead to reputational loss and legal liability, and being able to initiate and perform investigations before security incidents have an actual impact. Study participants commented on these benefits:

- **Reduce risk exposure by mapping potential threats:** *"We've leveraged DomainTools to identify our risk exposure . . . It's helped us identify and reduce risk by mapping out related threat actor infrastructures and putting in place mitigation steps or blocks so that they can't leverage it against us."*
- **Reduced risk of incidents through proactive detection:** *"Through the ability to detect malicious domains across our network, we're able to identify malicious activities sooner and respond before business or operational risk occurs. We can prevent the impact connected with*

a security incident. There's potential for reputational loss and legal liability if sensitive customer data is involved. We've reduced the risk of that happening by 25–33%."

- **Minimize operational risks and reduce fines:** *"We face large financial, legal, and business integrity risks, which we've reduced by about 20% with DomainTools . . . We've reduced fines because we can preemptively investigate something before it becomes a bigger risk. We've reduced them by around $100,000–200,000/year."*

More Effective Threat Investigation Teams

Study participants reported that security operations center staff responsible for threat investigation and response, including incident response and security analyst teams, work much more efficiently with DomainTools. This is enabled by having better and more actionable information available so these teams can stop threats from becoming full-blown security events that negatively impact or interfere with the smooth running of business operations. For study participants, enabling these teams to serve their businesses effectively and efficiently is a substantial benefit, both in ways that can be tangibly measured such as higher productivity levels and often more intangible ways such as reduced operational risk.

One key area where improvements were linked to DomainTools involved efficiencies for building risk score profiles for domains. To the extent that interviewed organizations even created risk profiles before use of DomainTools, it was often a cumbersome and time-consuming process. However, DomainTools has nearly automated risk profile creation. As one study participant explained: *"To determine a Domain Risk Score took 2–3 hours previously compared with 4–5 minutes with DomainTools."* Another study participant talked about better understanding potentially malicious actors: *"With DomainTools, we understand who controls a domain, and we're able to then find out what other domains they control. DomainTools allows us to hunt for specific hits that come from that source . . . Without it, it would take anywhere from 20 to 100 hours to build a risk score profile, and that's probably conservative."*

There were also several other ways that DomainTools helped interviewed organizations improve the efficiency of threat investigation team members, including having a single, more functional security platform. According to one study participant: *"Overall, our threat intelligence team is three FTEs . . . Without DomainTools, we'd add half an FTE and also two people at one-third of their time who are no longer working on a homegrown solution." Another noted: "With DomainTools, we need 10% of the 50 people for threat assessment. If we didn't have DomainTools, we would probably need at least 50% of the 50 people."*

Table 3 identifies and quantifies these efficiencies for threat investigation teams at interviewed organizations. As shown, substantial improvements were noted for security teams (24%) and incident management teams (28%), with other members of threat investigation teams seeing average efficiencies of 45%. Overall, this means that threat investigation teams at interviewed DomainTools customers are 34% more efficient on average. This represents significant value for study participants, saving or freeing up the time of more than eight team members, which IDC quantifies as having an average value of $836,100 per organization per year.

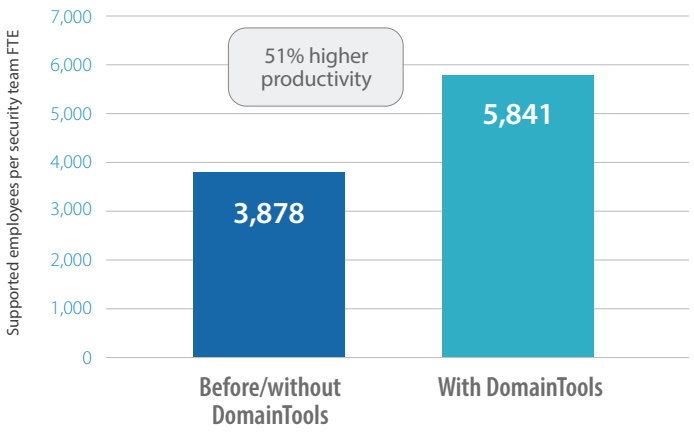
TABLE 3 Threat Investigation Team Impact

	Before/Without DomainTools	With DomainTools	Difference	Efficiency with DomainTools (%)
Incident management team	7.0	5.1	1.9	28
Security analyst team	7.6	5.8	1.8	24
Other threat investigation team members	10.2	5.6	4.6	45
Overall threat investigation team (total of categories)	24.9	16.5	8.4	34
Value of staff time required per organization per year for equivalent effectiveness	$2.49 million	$1.65 million	$836,100	34

n=6 Source: IDC, 2020

Efficiencies for threat investigation teams can also be viewed through the prism of their productivity and effectiveness. Figure 3 shows the extent to which these threat investigation teams' increased capabilities and effectiveness with DomainTools translate to higher productivity, which IDC quantifies at an average of 51% higher productivity. For study participants, this also reflects the much-improved security posture that they have achieved with DomainTools with the same threat investigation teams.

FIGURE 3 Threat Investigation Team Productivity Levels



n=6 Source: IDC, 2020

Business and Operational Impact

The previously described operational efficiencies that study participants derived from DomainTools also positively affect their business operations. As described, lowering operational risks associated with business activities provides confidence for interviewed companies to be more agile and limit concern about sustaining major financial and reputational losses due to data breaches. As one study participant explained: *"We have faster incident response and better visibility into threat intelligence with DomainTools. It enhances our overall business efficiency . . . Security doesn't directly drive revenue, but business units can be more efficient if they can stop problems before they generate expenses . . . I know for a fact that we have reduced disruptions. Whole business units have avoided incidents that could affect one to two thousand people."* While study participants generally found it challenging to place a value on these more intangible benefits of DomainTools, the impact is nonetheless real and reflects the extent to which their ability to limit operational risk instills confidence in business operations including the ability to make changes as needed to match changing demand.

ROI Analysis

IDC's analysis of the benefits and investment costs related to study participants' use of DomainTools is presented in Table 4. IDC calculates that, on a per-organization basis, interviewed organizations will achieve total discounted three-year benefits of $1.98 million ($4,490 per 1,000 endpoints) based on the security team's efficiencies and risk avoidance advantages described. These benefits compare with projected total discounted investment costs over three years of $0.48 million on a per-organization basis ($1,087 per 1,000 endpoints). At these levels of benefits and investment costs, IDC calculates that interviewed organizations will achieve a three-year ROI of 313% and break even on their investment in DomainTools in five months.

TABLE 4 Three-Year ROI Analysis

	Per Organization	Per 1,000 Endpoints
Benefits (discounted)	$1.98 million	$4,490
Investment (discounted)	$0.48 million	$1,087
Net present value (NPV)	$1.50 million	$3,043
ROI (NPV/investment) (%)	313	313
Payback (months)	5	5
Discount factor (%)	12	12

Source: IDC, 2020

CHALLENGES/OPPORTUNITIES

The basic technology that DomainTools uses is chasing down DNS queries and scoring domains based on proximity to badness; these cybersecurity approaches are not new. In addition, establishing lists of known good sites and lists of known bad sites is ostensibly laborious. DomainTools has established competitors such as RiskIQ (PassiveTotal) and Cisco Umbrella (OpenDNS).

However, when SOC teams go cybersecurity threat hunting, they can start building a case for triage. They can look for corrupted devices through memory cache intrusions and rule- or role-based violations, check for intrusion detection/intrusion protection (IDS/IPS) alerts, use user behavioral analytics (UBA), or monitor for data loss or file integrity management (FIM). At different times, any combination of these measures might be the proper procedures. Ultimately though, if the adversaries want to extract information, they have to contact an external server or website, or the adversary has to lead end users onto a malicious site so that they can download a phishing campaign or a ransomware attack. In this study, IDC found that, by starting with a risk score of unknown sites and investigating the factors that led to the elevated risk score, SOC teams were able to create more meaningful context that led to truer incident resolution.

CONCLUSION

The two universally recognized cybersecurity metrics are mean time to detect (MTTD) and mean time to respond (MTTR) to incidents. When a SOC is engaged, its most important capability is to quickly determine if a threat actor can actively exploit the network. In this study, IDC found that organizations inherently understood the need for domain risk scoring, and in some cases, organizations attempted to develop homegrown systems. The DomainTools Iris Investigation Platform data sets refine the processes that occur within an SOC to streamline investigations with guided pivots, risk scoring, and visualization tools. In addition, the DomainTools Iris Investigation Platform data set helps analysts determine the potential for future exploits based on threat actor infrastructure. These capabilities both serve to accelerate MTTD and MTTR.

IDC's research with DomainTools' customers demonstrates that security teams in these organizations generated measurable and positive results in combating adversarial activities. Most importantly, study participants reported substantially reduced risk associated with security events, incidents, and breaches through more proactive identification and resolution. While reduced operational and business risk can be challenging to quantify, the value for

interviewed DomainTools customers is real; they reported having increased confidence in their security postures and business operations. Further, they linked much higher productivity levels for their teams responsible for threat investigation to the use of DomainTools, noting that these teams can now carry out much more effective and targeted work regarding potential adversarial activities. Higher productivity levels for these teams, in addition to other staff time savings and operational cost reductions, deliver strong value to DomainTools' customers, which IDC quantified at an average three-year ROI of 313% with payback five months after deployment.

APPENDIX

Definitions

For purposes of this study, IDC used the following definitions:

- **Threat** is a circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.
- **Event** is an observable occurrence in an information system or network.
- **Incident** is an occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

Methodology

IDC's standard Business Value/ROI methodology was utilized for this project. This methodology is based on gathering data from current users of the DomainTools solution as the foundation for the model. Based on interviews with organizations using it, IDC performed a three-step process to calculate the ROI and payback period:

1. **Gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of DomainTools.** In this study, the benefits included staff time savings and productivity benefits and operational cost reductions.
2. **Created a complete investment (three-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using DomainTools and can include additional costs related to migrations, planning, consulting, and staff or user training.

3. **Calculated the ROI and payback period.** IDC conducted a depreciated cash flow analysis of the benefits and investments for the organizations' use of DomainTools over a three-year period. ROI is the ratio of the net present value (NPV) and the discounted investment. The payback period is the point at which cumulative benefits equal the initial investment.

IDC bases the payback period and ROI calculations on a number of assumptions, which are summarized as follows:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and manager productivity savings. For purposes of this analysis, based on the geographic locations of the interviewed organizations, IDC has used assumptions of an average fully loaded salary of $100,000 per year for IT staff members and an average fully loaded salary of $70,000 for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).
- The net present value of the three-year savings is calculated by subtracting the amount that would have been realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.
- Further, because IT solutions require a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC prorates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

Note: All numbers in this document may not be exact due to rounding.

IDC Research, Inc.

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC
ANALYZE THE FUTURE