DOMAINTOOLS®

POWERING INCIDENT RESPONSE BY OPERATIONALIZING THREAT INTELLIGENCE

"IF YOU KNOW THE ENEMY AND KNOW YOURSELF, YOU NEED NOT FEAR THE RESULT OF A HUNDRED BATTLES." — SUN TZU

When Sun Tzu wrote these iconic words, he couldn't have known how meaningful they would be for an altogether different type of battle more than 1,500 years into the future. Used over centuries by militaries, governments and businesses, his wisdom also speaks to the heart of cybersecurity—the art and science that practitioners perform from their desks every day.

In cybersecurity, learning about the adversary is the most important and effective way to protect critical information and assets. Knowing our enemies—who they are, where they are, what they do, their tactics, techniques and procedures (TTPs)—is the aim of every cybersecurity organization. The more we know, the smarter we are at defending ourselves. As an industry, we are under increasing pressure to do this better and faster.

Threat intelligence is the pathway that leads us to clear and actionable knowledge about malicious actors. The challenge with threat intelligence, however, is that while security teams have boundless access to both free and paid threat data feeds, they are often overwhelmed with information. The vast amount of data and alerts, combined with the resource shortage most teams face, makes it difficult to turn the data into intelligence that applies to the organization, and then translate that insight into actions that decrease the attack surface or address real, imminent threats.

More than half of organizations report a problematic shortage of cyber-security skills. The industry's global skills gap is forecasted to result in a record high of 3.5 million unfilled positions by 2021. Hiring more people is not currently an option for teams who are inundated with security data, alerts and incidents. Rather, practitioners need to operationalize threat intelligence, so they are empowered with better, faster, smarter ways to query, learn from and enrich threat data so it can be put into action.

"Security tools produce massive amounts of event data, which sometimes become security incidents. Teams need to enrich that data with cyber threat intelligence to give it context about the adversary's tactics techniques and procedures."

– Jon Oltsik, Enterprise Strategy Group

SITUATIONAL ANALYSIS

In an Enterprise Strategy Group survey of security practitioners, researchers looked at practices and challenges in threat detection and response (TDR) and how security teams are leveraging cyber threat intelligence (CTI). The findings paint a picture of the state of TDR and obstacles currently hampering efficiencies.

- Improving TDR is a high priority for more than 80 percent, particularly as the majority of cybersecurity practitioners feel pressure from executive management to do a better job.

- Despite the urgency from leadership, 74 percent said their organization's TDR is anchored by only a few key individuals. As the volume of intelligence, alerts and investigations scales, the internal experts that have the skills needed to effectively execute are increasingly overwhelmed.

- More than two-thirds said their TDR efforts are limited because they are built upon the use of multiple point tools. Teams receive a high number of alerts, but because they are not mapping the alerts and the data generated from each tool to the others, they lack context to understand the full scope of a particular event or indicator.

- TDR is viewed as more difficult today than it was two years ago by 76 percent. A number of factors are complicating this work, such as the sophistication of adversaries and a growing attack surface. Thirty-four percent cited the volume and sophistication of threats as the primary reason why things are becoming more difficult.

Cybersecurity workloads have increased for 76% of practitioners and the attack surface has grown 68%.

- More than 30 percent said their team spends most of its time addressing high priority/emergency issues and not enough time on strategy and process improvement. While this reflects on the skills shortage, it also reveals the gaps in current processes for effectively leveraging CTI to enrich event data.

CYBERSECURITY CAPABILITIES IN DEMAND

Many organizations are moving toward a cybersecurity platform that will help consolidate their tools. ESG asked the experts, "what are the most important attributes of a cybersecurity platform?" Their responses by the numbers:

38%
Security coverage that includes major threat vectors closely tied to DNS like email security and web security

33%
Central management and reporting across all products and services

31%
Provides threat prevention, detection and response capabilities

27%
Coverage that spans endpoints, networks and cloud-based workloads

26%
Cloud-based services

22%
Openness

20%
Platform made up of tightly-coupled plug-and-play products and managed services

18%
Offered in multiple deployment options

SITUATIONAL ANALYSIS (CONT.)

- The ability to compare what's happening on premises to what's happening in the wild is lacking for 24 percent. Without the tools and processes needed to compare imminent threats in the context of the overall landscape, teams are left guessing about the nature of their data.
- Twenty-three percent said security alerts don't provide enough context or fidelity for teams to easily know what to do with them.
- Teams are actively looking for solutions. Most (89 percent) are planning to increase spending—more than 50 percent said they will significantly increase spending.

These figures underscore the importance of operationalizing threat intelligence. Teams know they need to sort the wheat from the chaff to better understand their adversaries' networks and the TTPs they use. They remain mired in an overwhelming volume of disparate CTI and struggle to contextualize it and enrich it with other internal data. They need to prioritize threats according to their level of risk. They know threat intelligence can help them do this, but struggle to connect the dots.

EXTRACTING VALUE FROM THREAT INTELLIGENCE

Organizations are willing to spend more money on cybersecurity, but they want to understand the ROI. Teams who enrich and improve their threat intelligence, who shift their way of approaching the challenges, will see significant improvements in efficiencies and ROI. This requires operationalizing CTI. How? Action includes:

TECHNOLOGY CONSOLIDATION AND INTEGRATION

Most security organizations are using numerous analytics and operations tools, which often live in disconnected silos. The result is a "swivel chair" effect, wherein practitioners are continually pulled in diverging directions trying to follow and connect information from disparate systems. This simply does not scale. To effectively operationalize CTI and eliminate swivel chair operations, teams need a tightly integrated architecture in which the tools work together and consolidate the data intorobust intelligence.

Security Operations and Analytics Platform Architecture (SOAPA) is all about central integration of tools. It plays an important role in ensuring threat intelligence is connected to reporting and security telemetry across all products and services, as well as what's happening in the wild. This makes it so that CTI is indexed, made easy to query and presentable to the analytics tools in place. Then, teams have a bird's eye view and an easy way to pivot across the many data points to decrease the attack surface, enable effective TDR and improve prevention.

RISK SCORING

Organizations are shifting their investment away from buying more threat intelligence feeds to finding ways to derive more value from existing feeds. That value is associated with the ability to gain a deep understanding of the threats, actors and TTPs in the context of the existing security architecture. Risk scoring can help teams more accurately pinpoint if and how a threat is affecting their organization and whether further action is needed. DNS data is an important (and often underestimated) piece in determining a threat's risk score. It provides the information at the intersection of external threat intelligence, internal security telemetry and activity among cyber adversaries that are trying to disguise nefarious behavior as normal.

EXTRACTING VALUE FROM THREAT INTELLIGENCE (CONT.)

ADVANCED ANALYTICS

Analytics are important in helping overwhelmed analysts gather the breadcrumbs for their investigations and increase the scale of their work. AI and machine learning can help level one analysts with triage work, rapid detection and uncovering low and slow attacks that may be beyond their skill sets. The average poorly equipped team may complete around 10-15 investigations in a day, but with the right combination of analytics and consolidated CTI, that number can increase to 20-30 investigations per day. When evaluating analytics tools, it's important to consider whether a product caters to the needs and skills of both junior and highly experienced practitioners, so it can truly add value to the entire team.

PROCESS AUTOMATION AND ORCHESTRATION

Operationalizing threat intelligence extends to Security Operation Automation and Response (SOAR) as well. With formalized processes, coordinated incident response and automated workflows, teams can leverage the combined power of threat intelligence and SEIM systems, with a simplified way to fetch the right data at the right time. Within SOAR tools, threat intelligence can also be applied to automatic blocking for known malicious websites and IP addresses. This provides an advanced level of prevention at the perimeter, without requiring time and attention from the team to manually manipulate rules.

A REAL WORLD LOOK AT OPERATIONALIZING THREAT INTELLIGENCE

DomainTools Iris plays an essential role in operationalizing threat intelligence across the investigation journey for traditional red teams, threat hunters, incident responders and security operations centers.

The triage phase is particularly critical, the point in an investigation when teams are establishing: whether an incident occurred, what happened, the actual and possible consequences of the event. The team will also be classifying and prioritizing the next steps of the investigation. This is the point in which the context around threat intelligence becomes imperative. Having a process in place for triaging events is essential. Below is a glimpse at what the triage phase looks like in a real investigation using DomainTools Iris to operationalize threat intelligence.

"Our industry talks a lot about volume. But what's important is quality. Is the data timely? Is it detailed? If something is deemed malicious, we need to know why, and how that relates to the network." — Jon Oltsik, Enterprise Strategy Group

OPERATIONALIZING THREAT INTELLIGENCE (CONT.)

INSPECTOR VIEW

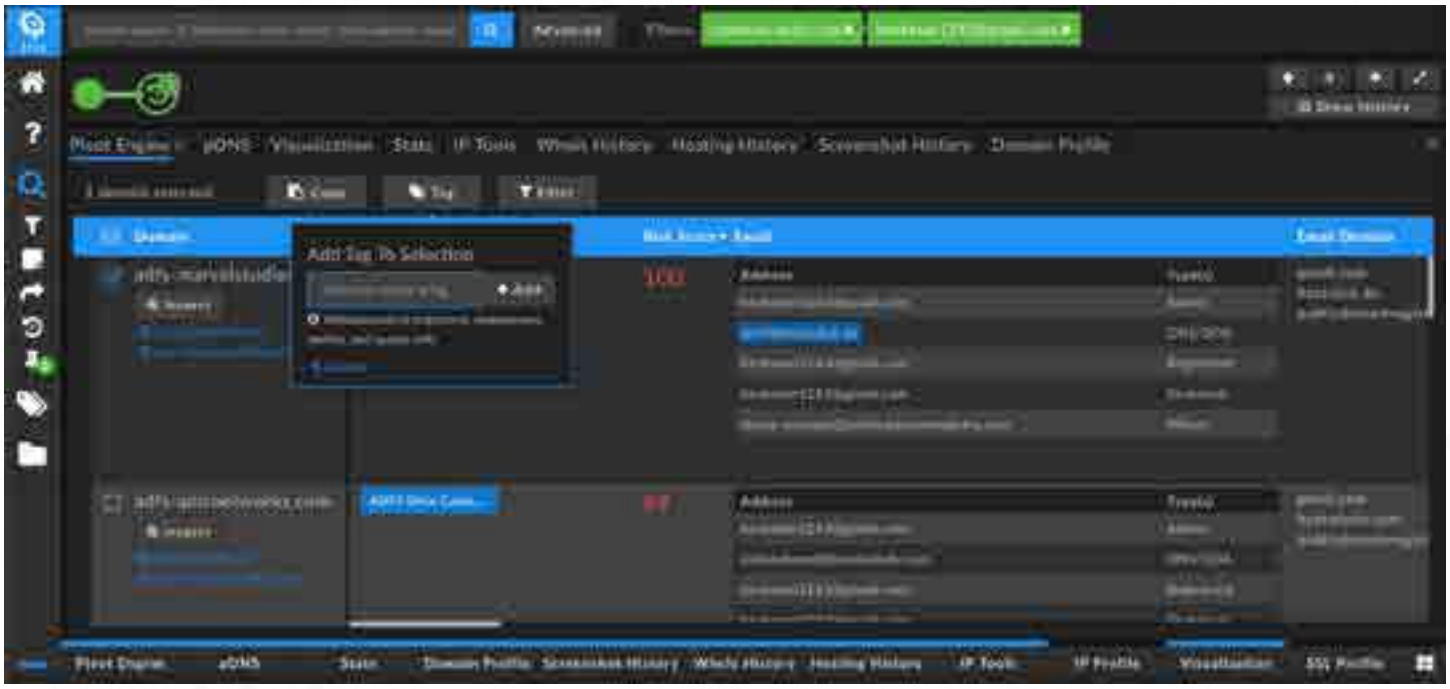
As the investigation begins, this interface provides a snapshot of known information. The Risk Score is a key component, and can be built out with additional information and context about a threat.

DOMAIN RISK SCORE

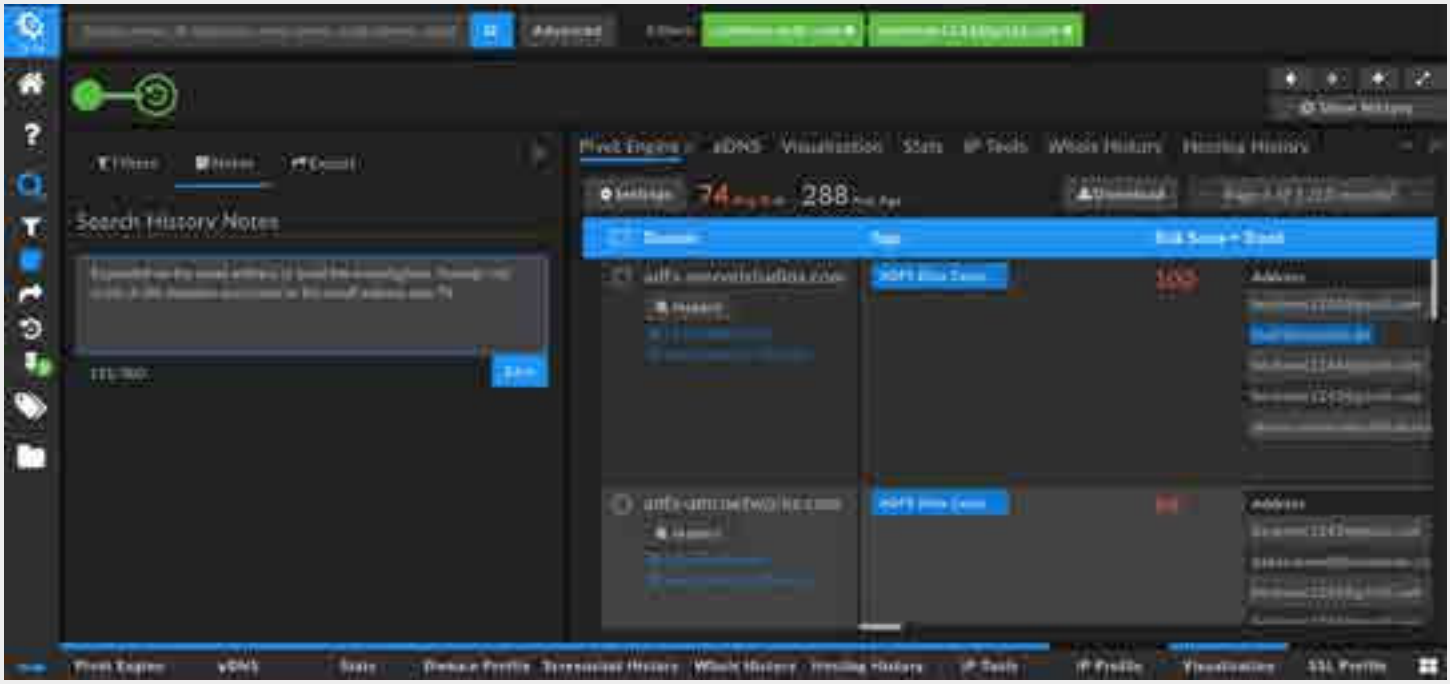
This is a predictive piece that can inform analysts of the likelihood that a certain threat is malicious, even before it is involved in an attack. This helps close the window of vulnerability between when a malicious domain is registered and when it is observed causing harm. Within DomainTools, a Risk Score of 0-99 means that the domain has not yet appeared on a blacklist. It also shows the threat's proximity to other sites that are known to be bad. It also includes a threat profile, which uses machine learning classifiers to determine whether a threat has the same behavioral characteristics as other threats such as phishing or malware. These insights offer context that can be turned into action in SIEM and SOAR tools and workflows.

PIVOT ENGINE

Using pivots identified in the inspector view, investigators can hover over certain data, such as an email address, to see other domains that share that same email address, and the average Risk Score for those domains. If it has a high Risk Score (anything over 70), the data can be expanded into the investigation, providing additional context and enrichment about all of the associated domains and IP addresses. This provides further opportunities to pivot and uncover key information relevant to the investigation.

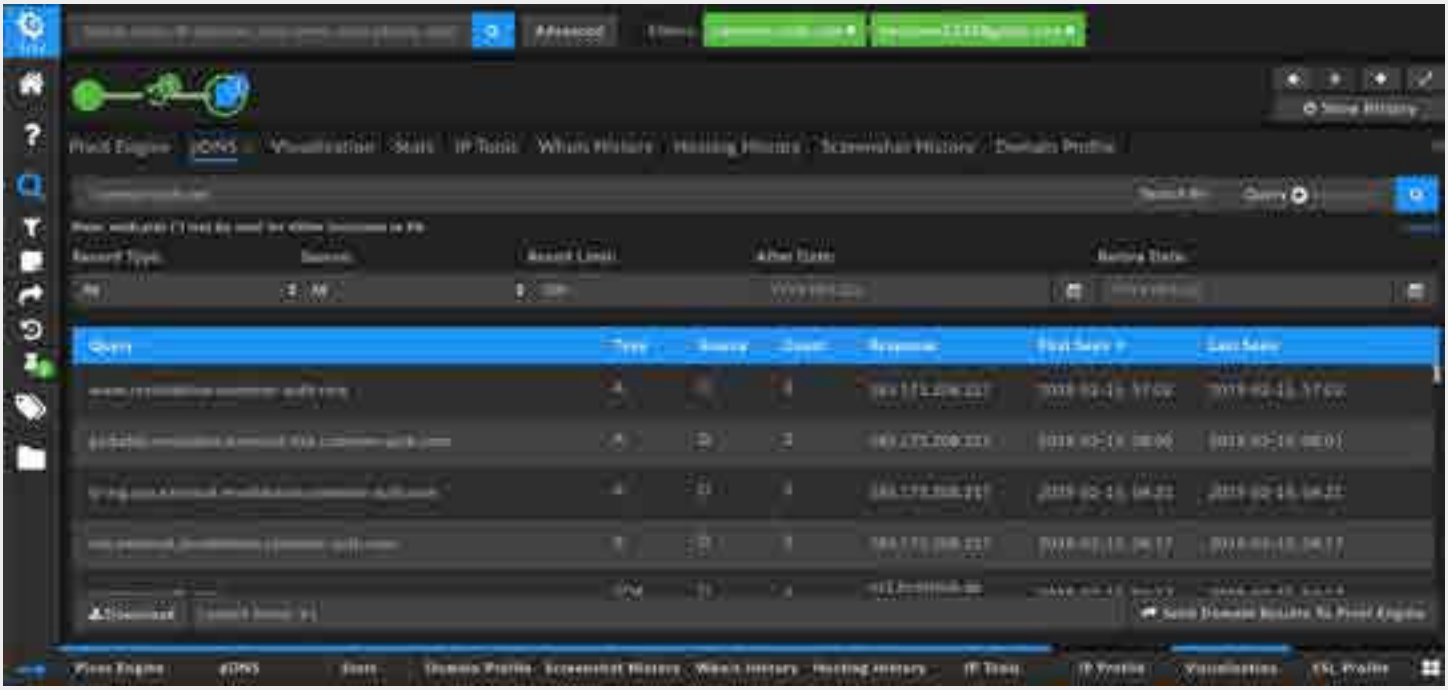


OPERATIONALIZING THREAT INTELLIGENCE (CONT.)



NOTES AND TAGGING

Throughout the investigation, researchers can add notes and tags to certain pieces of data. That way, as it is shared with team members or downloaded to STIX or TAXII, others can see what's already been done and why, and how it might apply to other ongoing investigations.



PASSIVE DNS

Iris turns passive DNS data into threat intelligence by allowing teams to integrate it into their investigations and compare which pieces relate to the threats under investigation. Teams can filter results in a variety of ways to build additional context. The results can be downloaded and added to the investigation with notes to explain the reasoning behind pivots.

OPERATIONALIZING THREAT INTELLIGENCE (CONT.)

VISUALIZATION AND STATS

With all of the data within the Pivot Engine, teams can run visualizations and generate stats that illustrate the connections between records, email addresses, name servers, etc., and the aggregation of threats under investigation. Results can be filtered by IP, country code and other classifiers to further build out the details of a report.

ENRICHMENT

The Enrich API in Iris was purpose-built for large-scale event data to help teams handle the rising number of events per second. With support for Splunk, QRadar and other SIEM tools, Iris can enrich proxy logs, DNS query logs, email domain logs and other data to help teams quickly surface malicious activity and reduce the time they spend on each event.

SOAR

Teams can work smarter, not harder with ready-made playbooks for incident handling and key workflows. This capability means teams are not forced into "swivel chair" syndrome, but rather can find the data they need or the next step in their workflow all in one place. Iris works with Splunk Phantom and IBM Resilient as well as other orchestration tools, to help manage vulnerabilities and reduce reaction time when containing harmful phishing emails and malicious network traffic.

"By integrating CTI with SOAR tools, teams can find the data and workflows they need all in one place, and escape the dreaded swivel chair syndrome."
– Corin Imai, Senior Security Advisor

CONCLUSION

Today's cybersecurity model is unsustainable. There are too many tools, too many processes and too little insight into what's happening in the wild. Things must change—so security organizations are enhancing the role of threat intelligence rather than becoming buried under a pile of feeds. The best threat intelligence is that which is timely, accurate, detailed, contextualized and easy to navigate. By looking at adversaries in an efficient way, understanding them and digging deeper with advanced tools, security teams can enrich their work and get on the most effective path to protecting their critical assets.