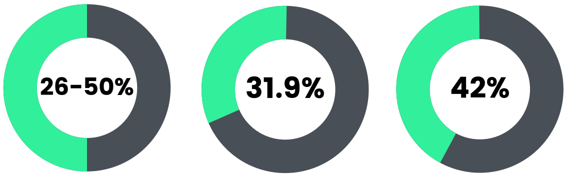
DTonomy

Reduce investigation time by 80% and eliminate risk with DTonomy's AI-based analysis and response

Are an ever-increasing number of alerts exceeding your security team's capacity?

- Are you overwhelmed by false positives alerts?
- Are you lacking enough resources to address every alert?
- Are you concerned that risks easily hidden in alerts can go undetected?

False Positives Causing Alert Fatigue



Alerts received by security professionals that are false positives

Security professionals ignore alerts because there are so many false positives

Cyber fatigue rose by 12% in 2020, to 42% of respondents

*according to McAfee and Cisco

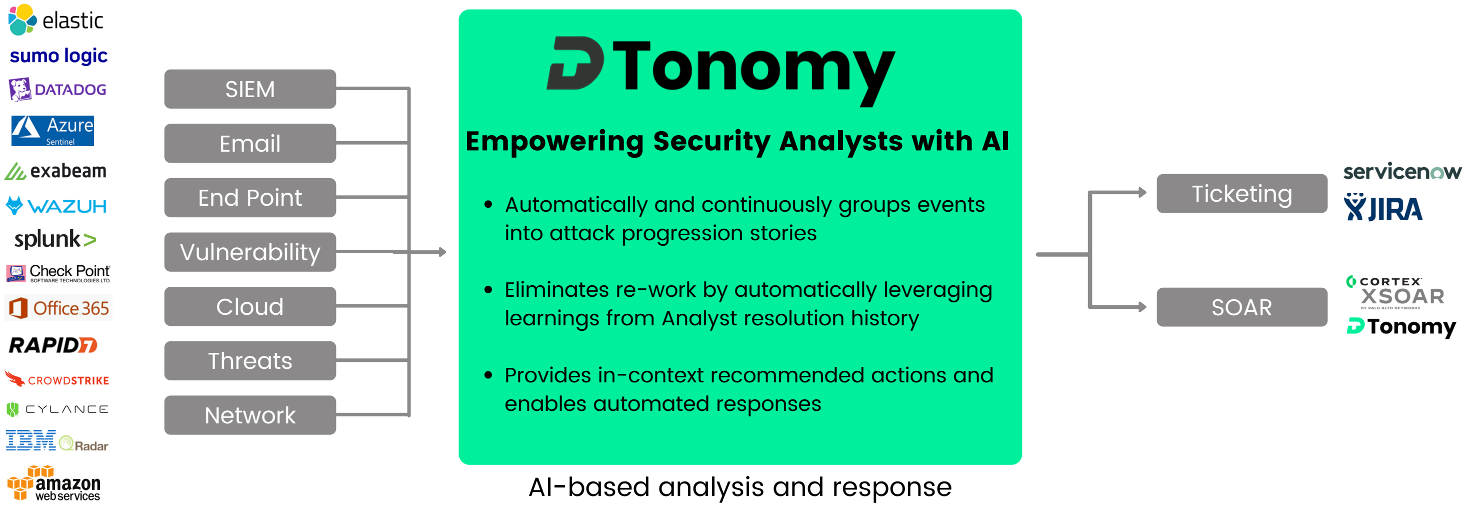
Too many alerts, too little resources

Modern cybersecurity teams are overwhelmed with alerts from a variety of user, system, cloud, application, and network-based systems. Most teams receive thousands of alerts every day, although large enterprises can receive millions daily. While these alerts are important for identifying indicators of risk, the average security team leaves 44% of all alerts to go uninvestigated, according to Cisco. Manually investigating and correlating all events is simply not achievable, given the amount of time and staffing required. High alert false positive rates, recently surveyed to be 26-50% of all alerts, also contribute to the large number of alerts that go uninvestigated. These alerts cause analysts to burnout, leaving their organizations at greater risk and struggling to replace highly sought-after skilled security professionals.

Artificial Intelligence (AI) to the rescue: hype vs. reality

While security companies have touted Artificial intelligence (AI) and behavioral analytics as the panacea to address these issues, AI has largely been limited to anomaly detection techniques, with the hope to reduce the number of false positive alerts teams receive. While the use of these AI techniques do reduce some false positives alerts, they unfortunately also create new false positives. This occurs with each valid change to user and system behaviors, which may be anomalous, yet create false positive alerts. As such, the benefits of AI for security have yet to be fully realized.

DTonomy applies AI in innovative ways to speed investigation efforts and upskill analysts



Empowering Security Analysts with AI

- Automatically and continuously groups events into attack progression stories
- Eliminates re-work by automatically leveraging learnings from Analyst resolution history
- Provides in-context recommended actions and enables automated responses

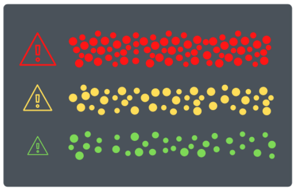
AI-based analysis and response

DTonomy's founders set out to build AI-based cross-correlation capabilities that instead of looking for anomalies, look for similarities in alerts. Doing this enables analysts with a smaller number of automatically-grouped alerts to review. As an example, instead of having to review 11,000 alerts per day, these alerts may boil down to 50 groups of automatically pre-correlated alerts.

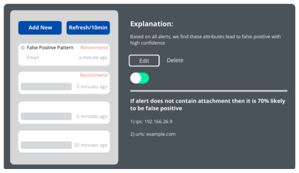
Besides reducing the number of objects that security analysts must review, the intuitive visualization of groups of related alerts speeds the analysis of the entire group and helps to expose the underlying system behaviors that caused them. Additionally, these new groupings are effective in enabling security teams to more quickly resolve the large numbers of alerts which are false positives. AI-based scoring techniques can be used to learn from security team decisioning to eliminate the need for security teams to regularly review the same groups of false positives on an hourly or daily basis.

DTonomy's AI-Approach to Security Analytics

Pattern Discovery Engine: DTonomy automatically cross-correlates alerts and presents them intuitively against the MITRE ATT&CK framework. By automating an effort that is otherwise a time-consuming, manual cross-correlation process, security teams can analyze significantly more alerts in less time. Besides reducing analyst efforts, this automation also reduces the risk that alerts requiring attention will go uninvestigated.



Adaptive Scoring Engine: DTonomy continuously collects feedback from users and provides customer-specific adaptive risk scores based on historic trends. This engine eliminates time spent repetitively reviewing false positives, enables focus on highest risk issues personalized to your environments, and identifies associated risks sooner.



False Positive Pattern

Email a minute ago

5 minutes ago

6 minutes ago

20 minutes ago

Explanation:

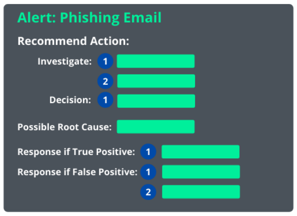
Based on all alerts, we find these attributes lead to false positive with high confidence

If alert does not contain attachment then it is 70% likely to be false positive

1) ips: 192.166.26.9

2) urls: example.com

Recommendation Engine: DTonomy provides relevant and in-context best practice recommendations. This engine enables actions to mitigate risk and close the loop on issues, increases analyst confidence in decisioning, and guides security teams to enable automations.



Alert: Phishing Email

Recommend Action:

Investigate: 1

2

Decision: 1

Possible Root Cause:

Response if True Positive: 1

Response if False Positive: 1

2

Automated Response

By performing more thorough and complete analysis, DTonomy is able to provide both meaningful in-context recommended actions and a playbook of automated responses. Automations enable faster responses to incidents, regular testing of security controls, consistent maintenance of allow and disallow lists, and eased security reporting.

Automated or Semi-Automated Responses - 100s of out of the box integrations can be used to easily create automations that speed the mitigation of risks.

Regular Testing of Security Controls - Ensure security controls are continuously operating as intended.

Orchestrate Interactions with Human Tasks - Enable seamless collaboration through integrations with tasking, ticketing, email, messaging, and other operational systems.

100+ Off the Shelf Integrations

DTonomy makes it easy to integrate with existing security technologies and tools. Out-of-the-box integrations, and our API-first architecture, enable security teams to collect and enrich alerts, as well as automate investigation steps and responses. DTonomy currently has over 100+ pre-configured integrations and is continuously expanding its list of integrations.

sumo logic WAZUH DEVO exabeam elasticsearch
CYLANCE CARBON BLACK FORTINET RAPID7 tenable
Gmail VirusTotal salesforce CORTEX XSOAR DUO
splunk> DATADOG Check Point Radar CROWDSTRIKE
Azure Office 365 JIRA servicenow aws
cisco Autotask Qualys. JS JavaScript Microsoft Teams

5-Star Customer Reviews

“Our customer environments generate many alerts, with DTonomy’s automated playbooks we are able to save time, provide more informed responses, and deliver better service to our customers." - Manager (Global MSSP)

“With DTonomy, we have gone from a highly manual process and many different systems to a one-click automated response, enabling us to respond faster and mitigate risk." - Network Security Analyst (Ivy League University)

Ready to reduce investigation time by 80% and eliminate risk?
Visit us at www.DTonomy.com