D3 SECURITY

XGEN SOAR

Key Features Guide

WHITEPAPER

A User-Focused Leap Forward for SOAR

The promise of SOAR is to make security operations faster, more streamlined, and more effective. So the last thing a SOAR buyer wants is to get bogged down in playbook-building, find out their tools don't integrate properly, get locked into rigid pre-built workflows, or otherwise end up wasting the time and resources the SOAR platform was supposed to help them save.

D3's latest release, XGEN SOAR, is the best realization yet of our approach to SOAR, which emphasizes making the user's life as easy as possible. It's not enough to provide a foundation of powerful technology. The platform must reflect the needs of security teams and help them achieve their most important goals.

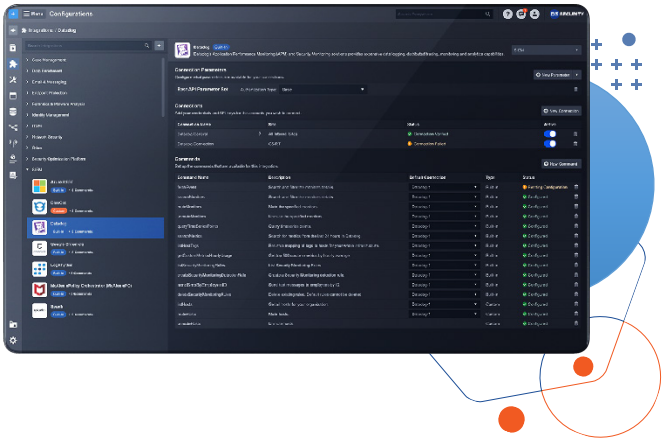
There are 13 key features in XGEN SOAR that demonstrate what makes D3 unique. These features are what enable D3's clients to:

- ✓ Hit the ground running with streamlined configuration.
- ✓ Spend less time building and testing playbooks and integrations.
- ✓ Connect to the widest range of third-party tools.
- ✓ Get a complete picture of the threats they face and the effectiveness of their security controls.
- ✓ Resolve incidents with agile playbooks that augment the skills of their analysts.

Unified Configuration

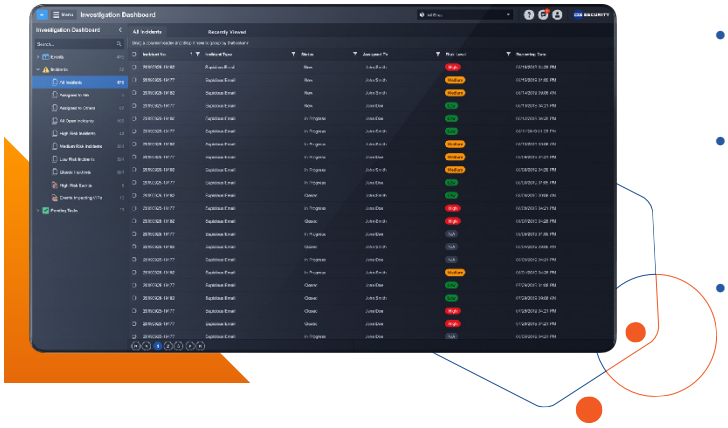
From the Unified Configuration screen, you can configure everything you need in one place: playbooks, integrations, utility commands, schedules, user permissions, and more. This makes it easier and faster than ever to set up and fine-tune your platform, without ever having to switch screens to find what you're looking for.

- Inputs are preserved in the left-side pane while you navigate across the system.
- User, groups, roles, and sites can all be managed in the User Management module.
- Transform data to build and test actions without leaving the configuration screen.



Dashboards

D3's dashboards provide an overview of event and incident data, pending tasks, and adversary TTPs. All mission-critical data is at your fingertips for at-a-glance management and—when needed—digging deeper.



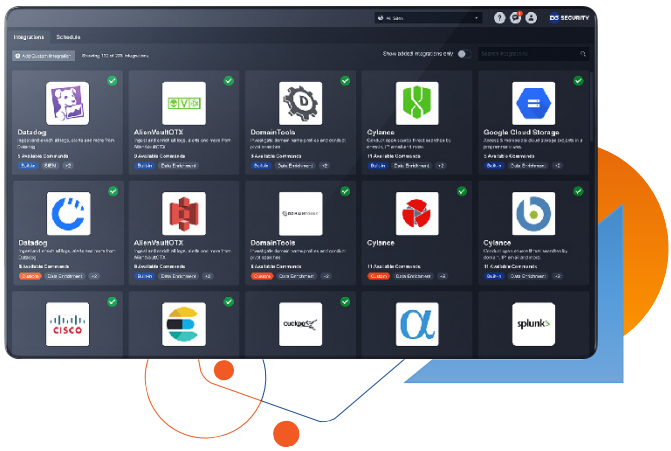
- Incident dashboards show a user-specific list of the status and severity of all incidents.
- Task dashboards show all pending actions in the system, along with their due dates, assignees, and associated incidents.
- The Monitor dashboard shows which TTPs have occurred in the environment.

D3 SECURITY

Integrations

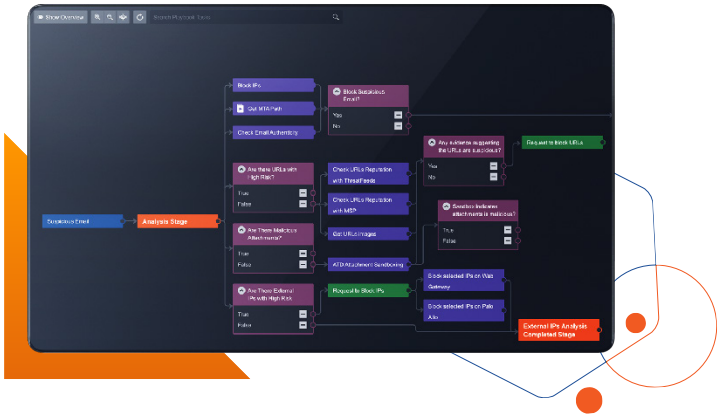
D3 integrates with more than 400 tools to orchestrate and automate actions across your entire security infrastructure. This simplifies security operations and accelerates incident response by connecting disparate tools and data silos through a single hub.

- As an independent vendor, D3 maintains the strongest possible integrations by working collaboratively with technology partners.
- Many integrations are bi-directional and fully featured, going far beyond what is possible through public APIs.
- Custom integrations and actions can easily be added by users.



Playbooks

D3's playbook library provides proven responses for the use-cases that every SOC need to be ready for. Resolve incidents fast and conclusively with workflows that are built to industry standards and customized to your exact needs.

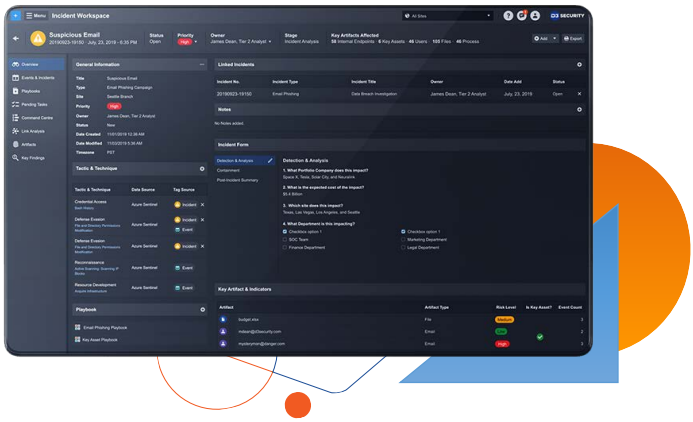


- Out-of-the-box playbooks based on NIST, SANS, and other frameworks.
- Automation-powered actions combined with human expertise.
- End-to-end workflows with unmatched customizability.

Full-Picture MalOps

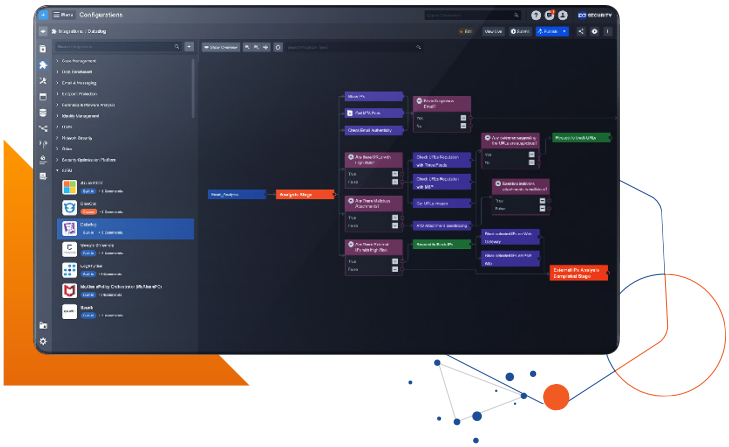
Malicious operations (MalOps) are high-fidelity incidents that bring together multiple events and rich contextual data into a single picture of an attack. Instead of tracking down all the pieces manually, you can quickly perform analysis and response on the entire attack, while continually expanding your understanding with new data.

- Visualize the kill chain of an attack.
- Automatically search integrated tools for relevant IOCs.
- Keep adding events and artifacts to the MalOp as the investigation evolves.



Low-Code Playbook and Integrations

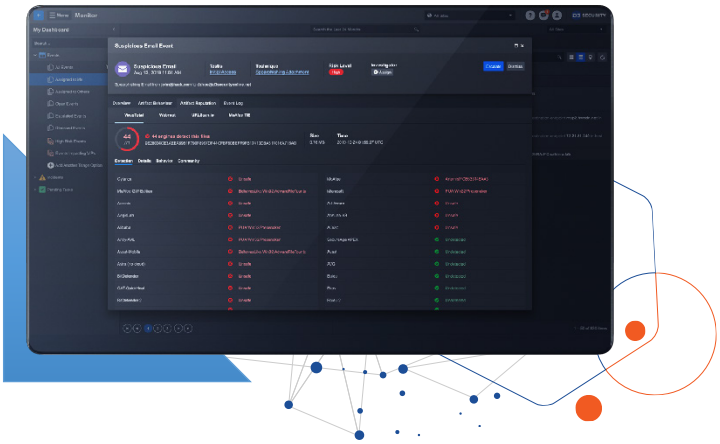
D3's Visual Playbook Editor makes it easy to create, edit, test, and publish automation-powered playbooks, complete with drag-and-drop orchestrated actions across tools. The low-code editor is intuitive and easy to use, regardless of your experience with coding, freeing up internal resources and empowering all users to build and optimize playbooks.



- Pick integrated actions from a searchable list in the left-side pane.
- Test entire playbooks, individual tasks, or individual inputs, all from the playbook editor.
- Build complex workflows, including loops, parallel actions, and dynamic contextual

Automated Enrichment

D3 automatically enriches security events using threat intelligence, incident knowledge, and MITRE ATT&CK data. You can eliminate the time wasted on manual intelligence lookups and quickly determine which events require immediate attention.

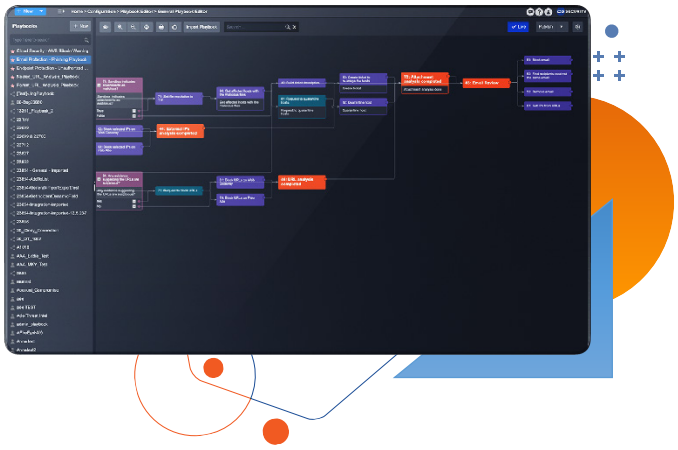


- The reputation of URLs, IPs, and more are automatically checked against integrated threat intelligence sources.
- Events are risk scored and queued based on findings.
- Likely false positives can be auto-closed or dismissed by analysts in a single click.

Response Orchestration

D3 ensures rapid validation and response to incidents by expertly orchestrating machine actions and human inputs. This enables rapid action across the entire environment without compromising flexibility or human oversight.

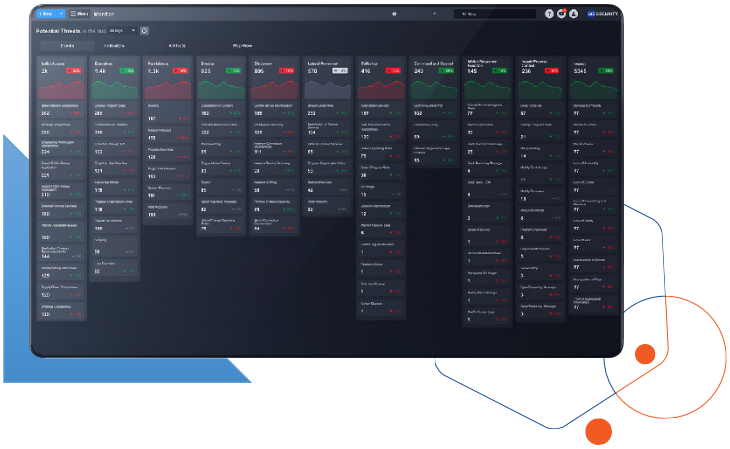
- Leverage more than 400 integrations to trigger actions, such as quarantining endpoints, blocking users, or updating firewall rules.
- Connect to tools via D3's Universal REST API.
- Reduce manual processes while retaining control over key decisions.



D3 SECURITY

MITRE ATT&CK Surveillance

D3 can search across past events and monitor future events for instances of important ATT&CK tactics, techniques, and procedures. This means you can automate the surveillance of the most pressing threats in your environment, knowing that you'll be alerted immediately when they're spotted.

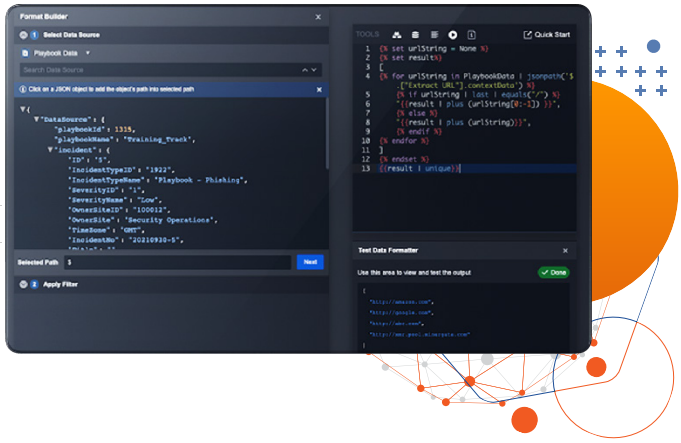


- IOC and TTP searches can fill in missing links in the kill chain.
- The Monitor dashboard provides at-a-glance view of all ATT&CK TTPs in the environment.
- Recurring searches can be automated in playbooks.

Jinja Template Data Formatter

With over 130 data filters, D3 transforms incoming data to make it easily usable for playbook building and testing. This eliminates the need for manual transformation or searching through mapped fields to find the data you need.

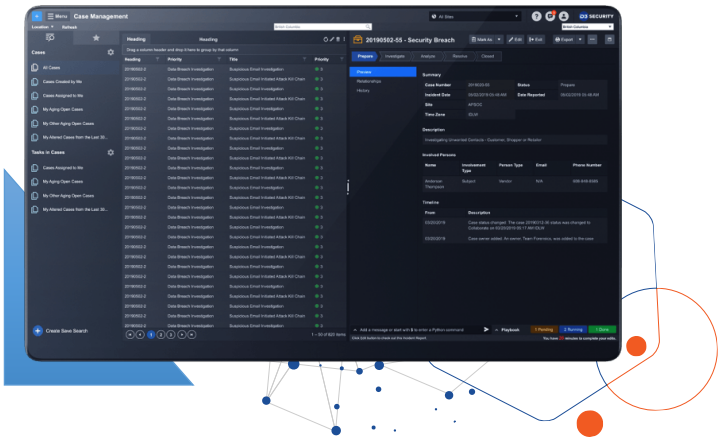
- Drill down into data sources and pull out entities or other data to build and test tasks.
- Instantly test new tasks from the playbook editor.
- Enable more complex conditional tasks.



D3 SECURITY

Investigation/Case Management

D3's case management capabilities include collaboration features, automated documentation of evidence and response activities, and granular access controls for sharing information securely. You can tackle complex investigations end-to-end with confidence, even when they expand beyond the SOC to involve other teams.

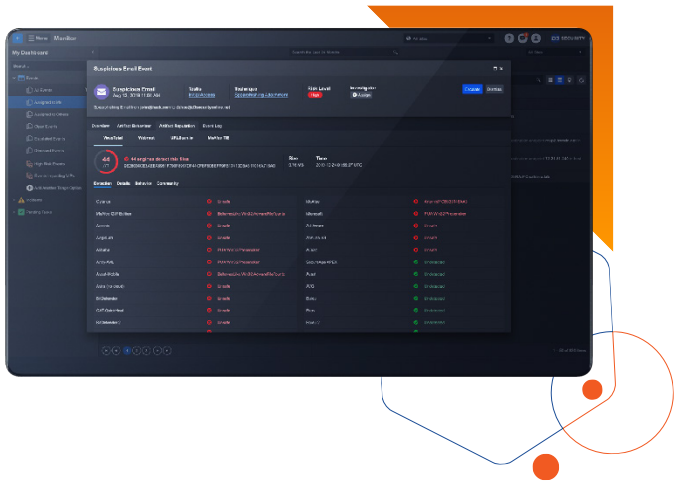


- Investigators can share notes directly in the timeline of an incident.
- Assign tasks, send notifications, and automate reminders to keep everyone on track.
- Related events can be grouped together for investigation.

Threat Hunting

D3 automates threat hunting across the entire environment via its 400+ integrations. You can save the time spent on slow, manual threat hunting, while ensuring that threat hunting doesn't get overlooked when your team gets busy.

- Turn ingested threat intelligence reports into threat hunts.
- Strip out IOCs from incidents and search for them across events, logs, endpoints, and more.
- Hunt for TTPs that are likely to follow in the kill chain of a detected attack.



SOC Metrics

D3 provides comprehensive SOC metrics that can be compared against predetermined benchmarks and turned into automated reports. By aggregating security data in D3, you can easily find and share the data you need, from simple analytics to compliance reports.

- Track MTTD, MTTR, incidents by type, and other important metrics.
- Assess analyst or team performance over time.
- Automate, schedule, and share reports, or save custom reports for reuse.

D3 SECURITY

D3 Security has been at the forefront of security orchestration, automation, and response (SOAR) since before the term was even invented. In this time, we've helped the largest companies in the world and early adopters from virtually every industry transform their security operations, incident response, and threat hunting.

This depth of experience has allowed to D3 to build the most comprehensive and scalable SOAR platform on the planet. It has also given our team members unmatched SOAR-specific expertise, which allows us to provide you—the person evaluating or buying SOAR—the best help possible.

We would love to discuss your automation strategy and show you how our product can help you achieve your goals.

JOIN THE NEXT XGEN SOAR DEMO

Email **info@d3security.com**

Follow **@D3Security on Twitter**

Connect **with D3 Security on LinkedIn**

Visit us online at **D3Security.com**

¿Quiere realizar una prueba gratuita del producto?

Argentina
Maipú 836 Piso 4
Teléfono: +5411 4783-0129

Uruguay
Antonio Costa 3578
Teléfono: +598 2622-2305

info@softronit.com
www.softronit.com