CrowdStrike Store

tines

CROWDSTRIKE

Data Sheet

TINES: ADVANCED SECURITY AUTOMATION AND RESPONSE

Intelligently automating security tasks and incident response (IR)

CHALLENGES

The complexity of keeping companies, customers and employees safe increases every day. Security teams are often overwhelmed with the need to manage multiple workflows across a myriad of tools. Tines simplifies the process of getting your tools to communicate, allowing you to automate key workflows and focus on the work that matters. Tines is an automation platform that enables your security team to automate repetitive workloads, making them more effective and efficient.

SOLUTION

When CrowdStrike and Tines are combined, all aspects of security operations and team culture benefit. Everything from alert enrichment to full-cycle incident response (IR) and compliance is enabled and automated. Tines also provides the CrowdStrike Falcon® platform with an immediate channel for integration into any customer's existing security investments or platforms (those that provide a RESTful endpoint/API) without requiring engineering development time. By embracing easy and flexible security automation, defenders regain time to move from a reactive to a proactive stance and can deliver a more resilient security posture across their organizational footprint.

KEY BENEFITS

- Enable your teams to build and deploy powerful workflows fast without writing code
- Automate repetitive security tasks and workloads
- Free up security talent for higher-impact projects, tasks and initiatives
- Rapidly build and automate full-cycle IR workflows
- Reduce alert fatigue, burnout and human error

TINES ADVANCED SECURITY AUTOMATION AND RESPONSE

BUSINESS VALUE

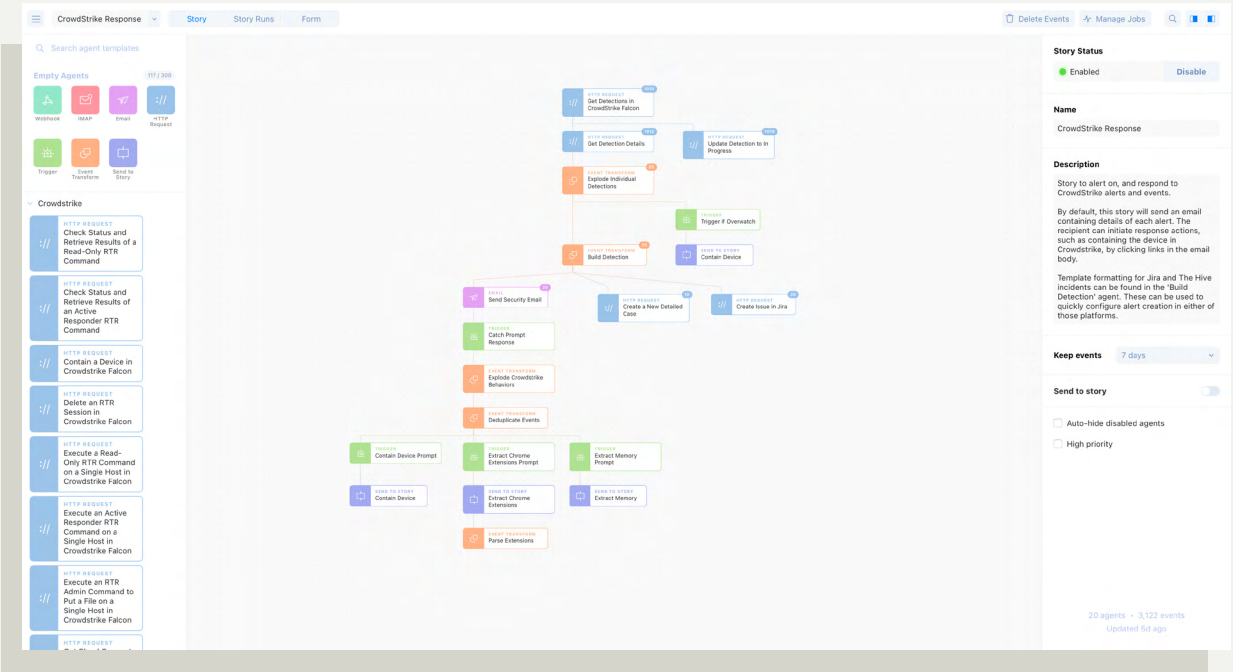
Use Case/ Challenge	Solution	Benefits
Combats alert fatigue, burnout and human error	Tines automates alert refinement, enrichment and validation. All associated repetitive low-value actions including basic decisions and responses are automated.	Errors are reduced and human talent is freed up to focus on more complex and challenging tasks and projects. Analysts, responders and engineers automate their basic workloads, enabling them to meet more strategic objectives.
Provides systematic and automated full-cycle IR	Tines story workflows allow for the automation of all facets of IR including automated endpoint interaction and even interactive engagement with users.	Consistent and rapid responses mean windows of exposure are closed and risk is minimized. Multiple endpoints, platforms and systems can be orchestrated and engaged for everything from low-level endpoint machine-based operations to setting up IR rooms and bots to assist responders.
Reduces mean time to respond (MTTR)	Tines works in internet time and at scale across all layers of orchestration for automated custom responses.	Immediate automated actions and workflows mean faster response times for validation, verification and remediation purposes. Dwell time is reduced, and responses operate at orders of magnitude faster than manual human actions could.
Provides alert enrichment, refinement and continual case management	Tines ingests alerts and operates on any alert field to deduplicate or refine data to actions. These story workflows transform alerts and enable reusable security logic.	Security teams gain the ability to operate at scale and overcome challenges with the volume of alerts. Tines reduces any noise and adds signaling that translates to automated actions. This security logic can also encompass and update third-party platforms such as case management, further freeing up human talent.

"Our success is built on automation, and that success is built on Tines. We've found that just one of our earliest implementations frees up 1.5 analysts per week. That's a lot of human hours that we can put into more complicated and professionally rewarding work."

John McSweeney
Director of Active Defence, McKesson

TECHNICAL SOLUTION

When you connect CrowdStrike and Tines, you empower full-cycle IR, additional threat intelligence and better context for all of your decisions and actions. Tines allows you to integrate easily with many local or remote data sources. You can quickly build workflows that leverage your preexisting processes, including those of other teams.



KEY CAPABILITIES

DRAG-AND-DROP STORY BUILDER

- The Tines Storyboard provides a drag-and-drop interface that allows security teams to visually **build automated workflows quickly** — up to 10 times quicker than equivalent, custom scripting.
- Automate any workflow using just seven multi-purpose components (agent types). Break the process you want to automate into individual steps, and use one of the seven agent types to perform that step (HTTP Request, Webhook, IMAP, Event Transform, Email, Send to Story and Trigger).
- **Not all security events are treated equally** — for example, a CrowdStrike Falcon OverWatch™ detection should be handled before a low-confidence DLP alert. High-priority stories ensure that the most critical security events are prioritized and handled first.
- Audit and record every action performed by Tines. Then use in-built reports, or create your own, to **demonstrate return on investment generated through automation.**

AGENT TEMPLATES TO ACCELERATE TIME-TO-VALUE

- The seven agent types can be configured to do almost any task, and **1,500+ preconfigured agents are provided** for actions commonly performed by security teams — for example, fetching detections from CrowdStrike Falcon® and creating a ticket in Jira. Agent templates dramatically accelerate time-to-value delivered by Tines.
- Create **private agent templates** specific to your institution that can be shared and accessed by anyone in the company.

DEPLOYMENT AND SCALABILITY TO MEET YOUR NEEDS

- In minutes, deploy Tines in the Tines-hosted cloud, or choose to deploy on your own infrastructure using Tines' lightweight containers.
- **Seamlessly scale to millions of automated actions per day**. Decoupled service architecture means that Tines can scale horizontally to handle any automation throughput.
- **Cloud-native support** allows security teams that already leverage services in public, private or hybrid clouds to easily deploy Tines using existing enterprise tools.

UNPARALLELED SECURITY AND RESILIENCE

- **Granular control over data residency and retention** ensures financial services institutions can easily meet even the strictest compliance requirements.
- Use the in-built Tines credential manager or leverage your own centralized secret management service to interact with third-party services.
- **Best-in-class error detection and story monitoring** ensure that if an unexpected event occurs, either inside Tines or on a supporting service, the right teams are notified quickly.

ABOUT TINES

Tines is an automation platform that allows security teams to automate their repetitive workloads, making them more effective and efficient. Tines, built by security practitioners and used by the world's leading security teams, is helping companies large and small to solve their most pressing security challenges.

Visit **Tines Docs** for more information on **agents**, **events**, **stories**, **credentials**, **globals** or **administration**.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 4 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**