Solution Brief

Automate Your Cloud Incident Response Workflow with the **Cado & Splunk SOAR Integration**

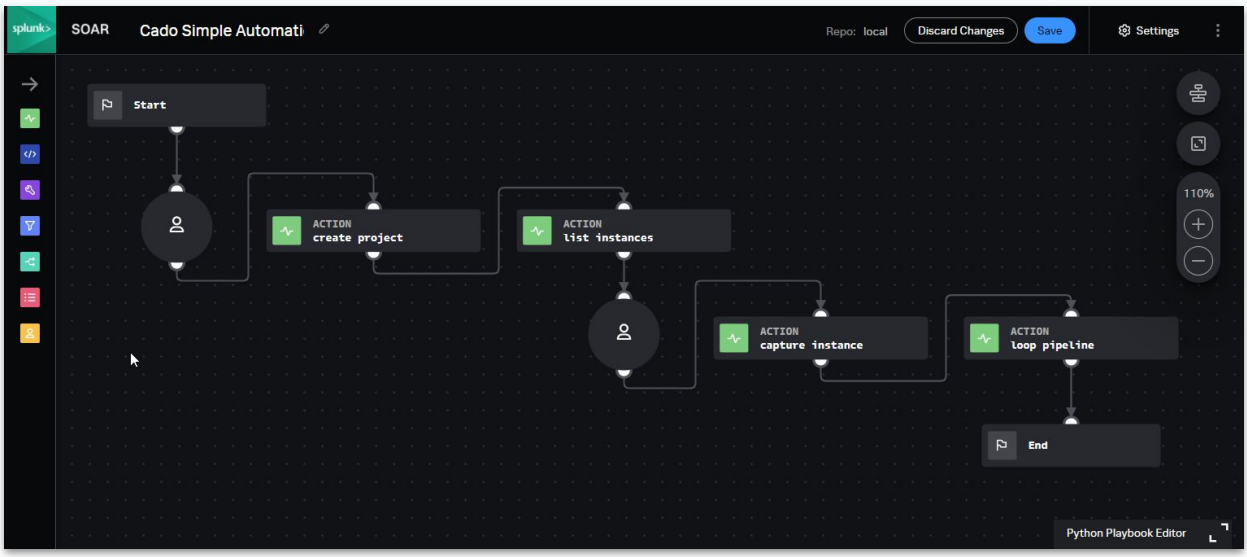
When it comes to investigating and responding to cyber incidents, one of the major challenges security teams face is getting the data they need when they need it. And the complexity of the cloud makes this task that much more challenging. Access often sits with multiple individuals or teams and evidence may reside in ephemeral resources, such as containers, or live across multiple cloud services and regions. When a high-severity detection fires, security teams need to move fast. The Cado and Splunk SOAR integration ensures analysts can get access to the data they need for an in-depth investigation without delay.

Joint Solution

The Splunk SOAR platform empowers security operations teams by automating repetitive tasks, implementing automated response actions, and orchestration to coordinate complex workflows across tools. The Cado platform delivers forensic-level detail and unprecedented context, taking the complexity out of cloud investigations. The Cado and Splunk SOAR integrated solution means security teams can significantly speed up their incident response actions and respond to threats at cloud speed.

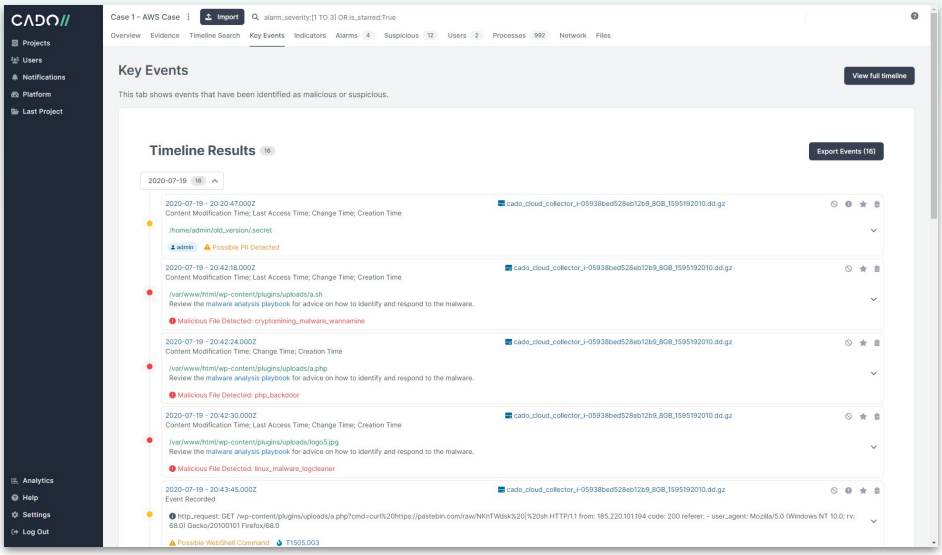
How it Works

By leveraging the Cado and Splunk SOAR Integration, security teams can customize playbooks to automatically capture critical incident evidence as soon as a malicious activity is detected. Following incident detection, Splunk SOAR will trigger the Cado platform to capture data across impacted cloud systems. Cado offers broad support, enabling investigations across multi-cloud and ephemeral container environments.



Cado is powered by a patent-pending architecture that automatically scales up and down to provide rapid parallel data processing, drastically reducing dwell time.

The Cado platform normalizes hundreds of different data sources across cloud-provider logs, disk, memory, and more. Data is further enriched using machine learning and threat intelligence and presented in a single timeline for immediate investigation.



Conclusion

The Cado and Splunk SOAR integration ensures critical evidence is captured immediately and automatically following detection. Kick off an in-depth cloud investigation without delay. Why wait? Speed up incident response, gain unprecedented context for investigations, and respond at cloud speed.

Key Benefits

+ Speed up incident response

Drastically reduce time to investigation and response.

+ Leverage automation to ensure incident data is captured before it disappears

Automatically capture critical evidence across ephemeral resources, such as containers, immediately following detection.

+ Gain forensic-level detail to understand the full impact of cloud incidents

Investigate hundreds of data sources across cloud-provider logs, disk, memory, and more.

Key Features

+ Multi-cloud coverage
+ Container support
+ Automated evidence capture

Cado Security is *the* cloud investigation and response automation company. The Cado platform leverages the scale, speed and automation of the cloud to effortlessly deliver forensic-level detail into cloud, container and serverless environments. Only Cado empowers security teams to investigate and respond at cloud speed. Backed by Blossom Capital and Ten Eleven Ventures, Cado Security has offices in the United States and United Kingdom. For more information, please visit **www.cadosecurity.com** or follow us on Twitter **@cadosecurity**.

CADO

splunk>partner+