April 12, 2018
FOR IMMEDIATE RELEASE

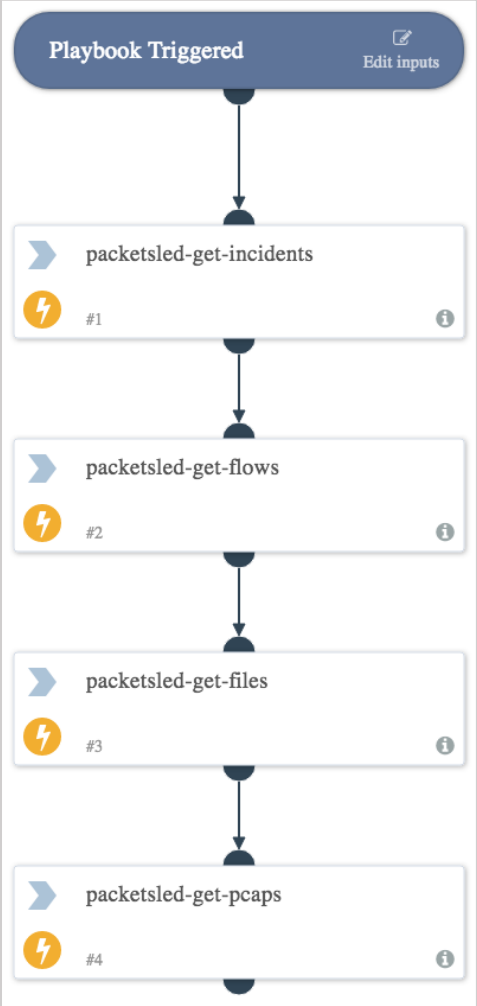
DEMISTO AND PACKETSLED INTEGRATE NETWORK VISIBILITY WITH WORKFLOW ORCHESTRATION

Demisto, the Leading Security Orchestration (SOAR) Platform, Partners with the leading Network Visibility and Threat Hunting Platform

SAN DIEGO, Calif. – April 12, 2018 - PacketSled, the leading Network Visibility and Threat Hunting Platform, today announced a partnership with Demisto, an innovator in Security Automation and Orchestration and Response technology. PacketSled will be rolling out a significant Demisto integration for customers looking for better ease of use in their security stack. PacketSled's Integration with Demisto enables customers and analysts to use PacketSled for workflow and deep-dive investigations. The PacketSled-Demisto integration accelerates Search and Investigation during the triage process by leveraging PacketSled's platform APIs and Investigative methodology.

Effective today, using a Demisto playbook, a practitioner can:

- Actively investigate network traffic based on simple search strings like IP address, hostname, traffic type and others across PacketSled indexes.
- Grab extracted files from PacketSled sensors for analysis using Demisto's orchestration playbooks in the same workflow.
- Capture and retrieve full packet capture using the same playbook, enabling SOC workflow from alert to raw data simply and quickly.
- Run PacketSled's API commands in real-time (along with 100s of other products) through a command-line interface for interactive investigations.



Collapsing multiple triage capabilities into a single playbook will enable rapid and decisive investigation and collection of immutable truth through Demisto and integrates into existing SOC playbooks, for use cases such as M & A, Risk Assessment, Continuous Monitoring or Information Rights Management.

The contextual viewing of data will also allow for quicker identification of remediation procedures and running the respective playbooks/actions to curtail the incident. Orchestrating security actions from multiple products in one window saves screen switching time, gives a better visual representation of alert data in one place, and enables further enrichment of individual sources through bi-directional integrations.

"We are looking forward to getting this into the hands of our clients, as it is a great move toward simplifying their workflow," said Rishi Bhargava, Demisto co-founder and VP of Marketing. "Demisto's award-winning platform is constantly improving the lives of our customers by integrating across the leading security products, such as PacketSled."

"PacketSled's exploration and investigation capability enables analysts and responders to gather forensic artifacts through Demisto's workflow. The orchestration of incident export, file extraction, PCAP analysis and triage through a playbook introduces SOC analysts to the simplicity of automation in workflow. As a critical platform component in the defender's tool chain, Demisto's PacketSled integration empowers analysts to investigate entities, automate evidence collection and context during investigations efficiently and easily," said Fred Wilmot, CTO at PacketSled.

###

About PacketSled
PacketSled is the leading platform for Network Visibility, Threat Hunting and Incident Response. Our network analytics platform automates incident response by bringing together business context, AI, entity enrichment and detection with network visibility. Used for real-time analysis and response, PacketSled's platform leverages continuous stream monitoring and retrospection to provide network forensics and security analytics. The platform is leveraged by response teams worldwide. Security analysts and SOC teams can integrate PacketSled's deep network context into their playbooks, SIEMs, or independently to dramatically reduce investigation time, cost and expertise required to respond to persistent threats, malware, insider attacks, and nation state espionage efforts. The company has been named an innovator in leading publications and by security analysts, including SC Magazine, earning a perfect score in the online fraud group test. The company has offices in San Diego, CA and Seattle, WA. For continuous product updates and industry news, please visit us at http://www.packetsled.com or follow us @packetsled.

About Demisto
Demisto Enterprise is the first and only comprehensive Security Operations Platform to combine security orchestration, incident management, machine learning from analyst activities, and interactive investigation. Demisto's orchestration engine automates security product tasks and weaves in the human analyst tasks and workflows. Demisto enables security teams to reduce mean time to response (MTTR), create consistent incident management process, and increase analyst productivity. Demisto is backed by Accel and other prominent investors and has offices in Silicon Valley and Tel Aviv. For more information, visit www.demisto.com or email info@demisto.com.

Press Contact:

KC Muir
Director of Marketing
(949) 742-4132
kc.muir@packetsled.com