For Immediate Release

SIEM Incident Response Platform Demonstrated at RSA Conference by D3 Cyber

D3 Incident Response Platform integrates with HP ArcSight, Splunk and IBM QRadar SIEMs

San Francisco, Calif., March 1, 2016 – D3 Cyber, the leader in incident response and integrated SIEM case management systems, today announced that it will showcase its SIEM integrations—including HP ArcSight, Splunk and IBM QRadar—at RSA Conference 2016, March 1-3 at the Moscone Centre in San Francisco, Calif. At D3 Cyber's booth #N3140, conference attendees can visit demo stations for HP ArcSight, Splunk and IBM QRadar, and see first-hand how SIEM integration can accelerate incident response, enforce playbook-driven standard operating procedures, and streamline investigative workflow through the D3 Incident Response Platform.

- At D3's **HP ArcSight** demo station, RSA attendees can automatically create incident records complete with threat agents like organization name, IP, and malware type; trigger NIST-compliant incident response playbooks; model threat agents and perform link analysis in D3. Additional case management capabilities include documentation of evidence sources and one-click escalation to digital forensics review.

- At D3's **Splunk** demo station, RSA attendees can customize their search parameters or leverage D3's turn-key filters for source IP, destination IP, source MAC address, destination MAC address, source port, destination port, host ID/host name, by tag, and by rule. Notable events can trigger incident records or incident response playbooks, while multiple incident records can be consolidated into a single D3 investigation/case.

- At D3's **IBM QRadar** demo station, RSA attendees can trigger both incident response and incident investigation workflows. Both QRadar and X-Force threat intelligence enrich incident response workflows with actionable data, enabling informed response, increased contextual awareness, and a searchable database of artefacts, threat intelligence and incident records.

"By unifying these leading SIEMs with D3's incident response platform, organizations can extend their case management workflow to the frontier of risk," said Gordon Benoit, president, D3 Cyber. "The result are organized and filterable intelligence streams that empower organizations with deeper contextual analytics, as well as prescriptive playbooks with granular task profiles."

In addition to SIEM integration, core components of the D3 Incident Response Platform include a threat intelligence hub, playbook library and digital forensics case management system. D3's library of incident response playbooks are built upon the NIST 800-61 framework, enabling NIST-compliant incident planning, plus custom playbooks that infuse foundational NIST templates with team-centric best practices.

About D3 Cyber

D3 Cyber provides an Integrated SIEM and Incident Response Platform to thousands of users, including 100+ of Fortune 500 companies. Our award-winning incident response platform unifies SIEM integration, threat intelligence hub, playbook engine, NIST compliance, and digital forensics case management. Available on premise

or SaaS, all D3 solutions are modular, customizable, and easily scaled. Best of all, each customer is supported by a dedicated business analyst and the D3 Customer Success Team.

Contact D3 Cyber or call 1-800-608-0081 Ext. 2

For press inquiries, contact:
Alex MacLachlan
Director, Marketing & Communication
D3 Cyber