Benefits

- Playbook driven triage and remediation of application level security events
- Expose production security events to operations and development teams
- Correlate event data across multiple data streams improving accuracy and context
- Detect application level attacks and block from the network

Overview

tCell and Demisto close the interoperability gap within development, operations, and security organizations (DevSecOps). With increased visibility within the application and context of what attacks are happening, companies are able to protect their web applications and API services by quickly remediating and blocking these bad actors and actions in real-time.

With Demisto you are able to design and deploy custom security rule sets based on the rich data provided by tCell’s RASP solution.

tCell And Demisto Integration Provides

- Deep visibility and insight into OWASP Top 10 style attacks through tCell’s cloud based analytics platform
- Remediation via Demisto’s playbooks and automation scripts
- Correlation of XSS data feeds with tCell’s Content Security Policy tool and DOM based instrumentation
- Promotion of cross-team collaboration with webhook alert integration
Challenge: In an industry controlled by regulations and compliance, healthcare organizations need tools that quickly deliver protection against software attacks and breaches. Collaboration between development and security organizations have been the biggest hurdle for speedy remediation.

Solution: When an attack is detected by tCell, Demisto quickly runs a playbook defined by Veeva to start the process of remediation. The required teams are identified, tickets are created, and developers have contextual data to fix any holes rapidly. When more information is required Demisto is able to enrich the attack data to find any correlations between multiple data streams.

Additional Benefit: Security and incident response teams need actionable intelligence. The combination of tCell and Demisto allows Veeva to cut through the noise and act in a timely manner.

ABOUT tCELL

tCell moves application security out of the network for cloud-first organizations. Using advanced Runtime Application-Self Protection (RASP) functionality, tCell secures web applications in production using server-side instrumentation, browser-side instrumentation, and cloud-based analytics. tCell is the only solution for companies leveraging DevOps, Agile, or micro services to protect their applications without code or network changes. Whether applications are on-premise or cloud-based, tCell’s unique approach makes application security easy. For more information visit www.tcell.io or email sales@tcell.io

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 resolution (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.