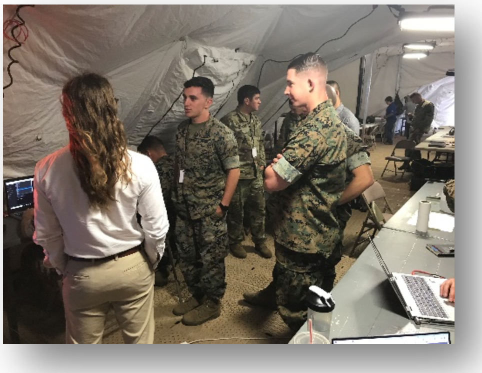
Driving Innovation: Integrating Technology & Developing a Tactical Solutions for the Battlefield

ITG Cybersponse SOAR Tactical Solution Army Cyber Quest 2019

Integration Technologies Group (ITG), in collaboration with **CyberSponse**, has integrated technology from several **leading cyber security firms** to provide the US Army with an **innovative tactical solution**.



The **Army Cyber Battle Lab located in Ft. Gordon, GA** has recently released their official assessment report. After an extensive review, several companies were selected to test their solutions in the lab. After successful testing, **CyberSponse was then selected to be deployed in the field while supporting Army Cyber Protection Team soldiers of the 101st Airborne Division** this past June.

When deployed at the battalion and brigade level, this solution can provide real time inspection, identification of malicious code or actors, and automated response capabilities. It requires minimal training for soldiers and a small data form factor platform that can be deployed quickly.

It relies upon several industry leading technologies to deliver a capability not previously available to tactical units. These include:

- **CyberSponse CyOps – SOAR** - Security Orchestration and Automated Response package,
- **Integration with end user operating systems**,
- **API level integration to Army Program of Record COTS products** (PAN, Splunk, End Game, Elastic, Red Seal, etc).

The US Army identified several requirements for the operating field environment:

- **SOAR**: Ability to ingest from current DoD Systems (CYBERCOM, CNMF, Pentagon); future integration points via robust API and flexible development team; out of box response capability and playbooks to block, neutralize, deceive, and redirect across the network; endpoint and cyber technologies
- **Hardware**: Virtualized solution can operate on currently certified, program of record HW at the tactical edge (PacStar / HPE) OR on current server architecture

The Army specifically mentions in their report about CyOps:

Objective 1

Determine whether the SOAR tool can integrate with the existing Program of Record (PoR) environment to deter or defeat enemy (Red Team) Offensive Cyber Operations.

Overall Observations / Comments:

- **Cybersponse CyOps successfully integrated with all of the specified Program of Record (PoR) systems** within the Experiment Environment. Engineers demonstrated significant flexibility and skill to adapt the tool to the requirements of the various PoR tools.
- **Cybersponse CyOps successfully orchestrated responses to the simulated cyber threats**. There were no shortcomings of the tool in this I&T event.
- Due to successful integration, **Cybersponse CyOps was able to demonstrate formatting, correlation and alignment of threat data to generate response action**. Operators also commented on the user-friendly UI.

Objective 2

Determine whether the SOAR tool can improve the economy of force applied to DCO by providing a case management capability.

Finding:

- **CyOps successfully achieved all criteria within Objective 2** and has the functionality to support existing Cyber Protection Team case management procedures.

Objective 3

Determine whether the SOAR tool can deter or defeat simulated enemy OCO by identifying anomalous activity on the tactical network.

Observation / Finding:

- **CyOps provided an additional function which allowed the conversion of time formats**. This was useful in that it enabled the user to correlate anomalous activity, which took place simultaneously on systems operating with different time stamps
- CyOps contains the required functionality to successfully deter and defeat Offensive Cyber Operations in the existing tactical Program of Record environment.

Objective 4

Determine whether the SOAR tool can retain key cyberspace terrain in the tactical network by orchestrating and automating an effective response to simulated enemy OCO.

Finding

- The tool responded successfully to simulated cyber-attacks and prevented staged ‘Enemy’ OCO operations in the BCCS environment.

Overall observations

- **Cybersponse's CyOps tool successfully achieved all experiment objectives in four days** against the allocated five day I&T window.
- CyOps' successful performance can be attributed to the inherent quality of the tool and the approach of the Cybersponse engineering team.
- **Integration was a smooth, well-planned activity and results were correspondingly good**.

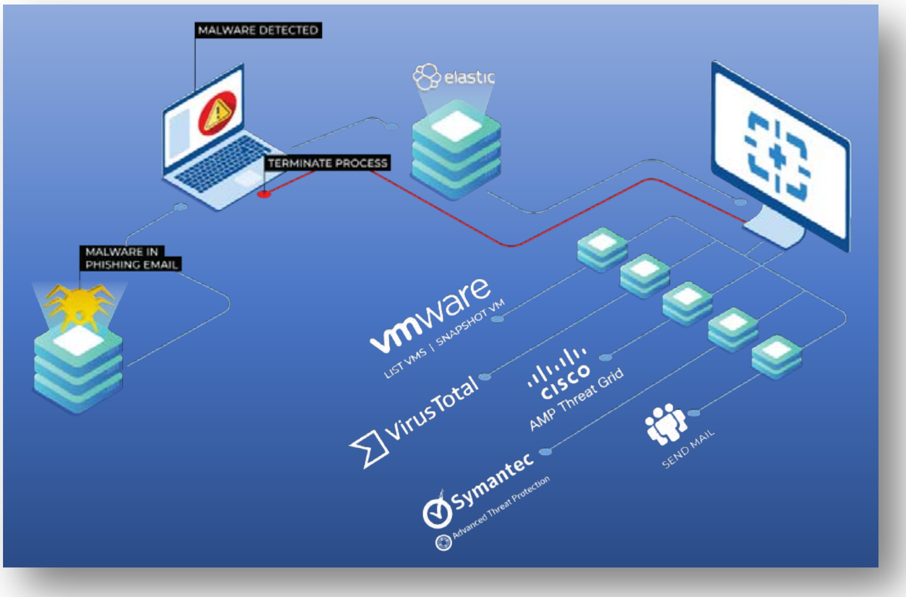
Key Benefits to Army Cybercom

During the 2019 Cyber Quest exercise, like most organizations today, the Army defined their key concerns as manpower availability and were interested to see if SOAR could help alleviate this concern. From the Army report:

The Army has limited cyber defense resources. Skilled personnel spend the majority of their time parsing log information and sorting through multiple false positive alerts, before they can actively hunt threats and identify confirmed intrusions into tactical networks. SOAR tools have the potential to reduce the time that network defenders spend sorting through logs and discounting false positives.

CyOPS Solves Major Manpower Issues through Automations

Drastically reduced times to remediation means soldiers can do more in the same time. A SOC analyst or CPT soldier will have their hands full when it comes to keeping up with the monumental volume of events - they must identify, prioritize and address only the most critical ones.

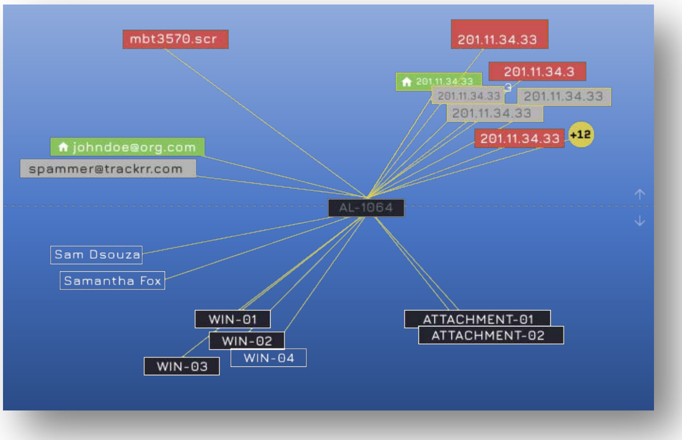


Volumes of events should not become a limiting factor for SOCs to compromise on the quality of service (QoS) and client expectations. A SOAR solution solves this problem by helping organizations to address the skills gap and ease the analyst's manual workload by the automation of playbooks and workflows. SOAR has emerged as the leading solution to allow organizations to effectively and efficiently reduce their overall security risk.

In addition, the time and cost of onboarding new team members is a major frustration that analysts face every day as it involves familiarizing new personnel with all security products/procedures and then ensuring that they reach a point where they can contribute effectively.

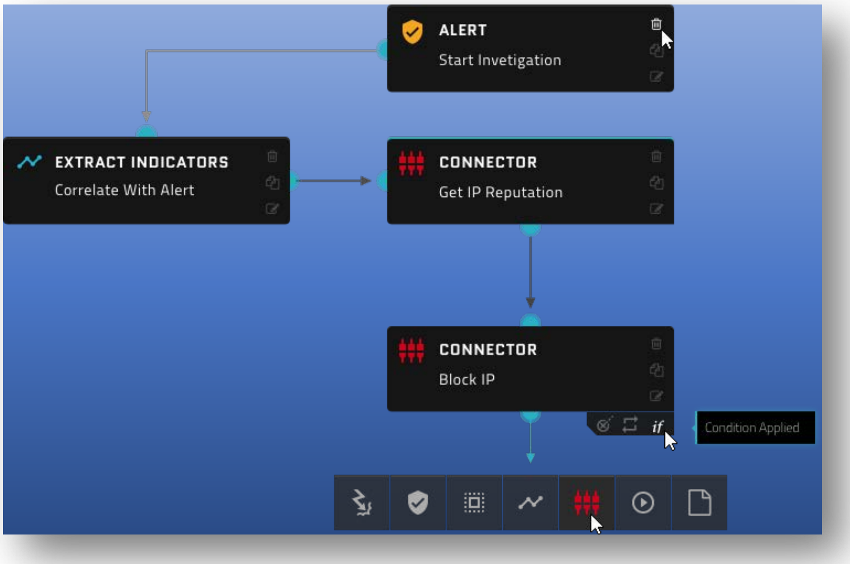
Proactive Threat Hunting

In using orchestration and automation techniques, an analyst can rapidly coordinate among multiple security tools. SOAR enables SOC team to ingest threat feeds from multiple sources and automate workflows to proactively scan potential vulnerabilities across environments.



Visual Playbook Builder

Drag and Drop **NO PYTHON CODING SKILL REQUIRED**



Leverages Knowledge

Enabling soldiers in the field to deal with complex problems and ensures they complete every required step in the process.

Reduced False Positives and Improving Investigation Quality

SOAR tools can help improve the quality of an investigation by enabling faster resolution of false positives. Analysts typically spend a large portion of their time in annotating and re-mediating false positives. By bringing automation up to 80 percent, security analysts' time can be freed and hence utilized to learn the detailed vernacular of many security products.

Intelligent Reporting and Creating a Knowledge Base

In most of the SOCs, analysts spend a large amount of time managing cases, creating reports and documenting incident response procedures. By collecting intelligence from multiple sources and presenting this information via visual, custom dashboards, SOAR can help organizations reduce paperwork while improving communication channels between the CXO's and the analyst. By automating playbooks, SOAR also helps to create a knowledge base and avoid loss of intellectual property and institutional memory, something that can happen all too easily given the difficulty organizations are facing in retaining security talent.

Conclusions & Key Differences provided by this Integrated Solution

- The 2019 Army Cyber Quest demonstrated that this technology is field ready for our soldiers today. **Our engineers provided hands on training and advised the team**. As a result, **soldiers effectively leveraged this important technology to quickly remediate and stop attacks**. In addition, the playbooks they developed can be shared and used easily by any other soldiers in a deployed environment.
- The ability to leverage knowledge from more experienced soldiers across the battlespace allows the Army to **train faster and improve the effectiveness of its soldiers**. Using advanced automation has a multiplier effectively turning one soldier into 6. By using this SOAR technology, **we can address the Army's manpower and knowledge/training issues in a fast and effective way.**
- **Playbook development doesn't require any code skill** (i.e. no Python required).
- **Significantly reduces time to remediation** and ensures all required actions are completed in compliance with Army standards.
- Uses flexible, open API and connectors to ingest any output to **over 600 current technology partners.**
- **Leverages cutting edge analytics to enable accurate classification** and actioning of lower threshold alerts (AD, ACAS, HBSS, ESM, etc.) and static code analysis with content/malware integration.
- Conducts analysis and holds data at the lowest levels in a distributed model in a manner that conserves bandwidth, leverages local processing power, and allows defenders to conduct remote response actions from anywhere within the network.
- **Ability to configure and distribute sensors and analytics from higher HQs to tactical units**.
- **Provide IOC distribution and use observed enemy TTPs to help enable OCO focus and response actions**.

If you would like additional information or a copy of the official report, please contact:

John Malyevac, Business Development Manager, Cyber Specialist,
John.malyevac@itgonline.com | (703) 698 8282 | (703) 622-1644