Cyber Security Operations Platform

Continuous Challenges Faced by the Industry

Expanding adoption of the latest digital technologies creates both opportunities and increased cyber risk. Security practitioners must assess new technologies' potential security impact on the network and educate themselves on the new environment.

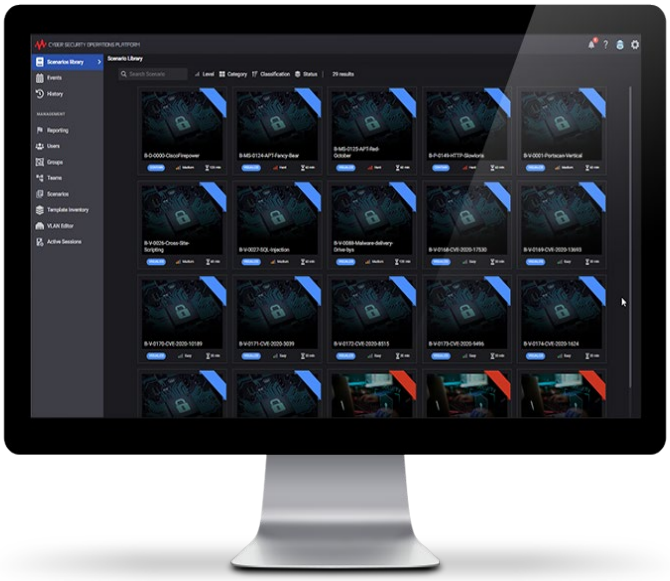
Private businesses as well as government bodies are responsible for protection of their technology, sensitive data, and intellectual property. To support this, organizations must have solid policy and procedure requirements that enable risk identification, prevent data compromise or theft, and provide an appropriately effective response when incidents occur.

Security professionals are required to be workforce-ready from day one and be able to contribute to the team effort of reacting to every incident. Classroom training and tabletop exercises do not adequately prepare front-line security employees with the ability to effectively detect and manage the complexities of an actual cyber incident. Security teams often train on security attacks that are unrelated to their current network infrastructure, day-to-day tools, and processes.

As a result, the need for hands-on experiential learning has expanded. This type of learning enables security professionals to practice realistic attacks and defense responses in a simulated environment, as well as explore ways to mitigate cybersecurity risks.

Highlights

- Easy-to-use solution for cyber security assessment
- Multi-tenant architecture
- Security tool agnostic
- Predefined and customizable threat scenarios
- Real-world simulations using Keysight tools (optional)
- Capture the Flag events promote increased team collaboration



KEYSIGHT

Our Solution: Cyber Security Operations Platform

Keysight's Cyber Security Operations Platform is a complete solution that provides a controlled protected environment for security professionals to gain hands-on cyber skills and to test the organization's security posture. The solution consists of:

- **Cyber Security Operations Platform** – the solution foundation with cyber range orchestration, management, reporting, platform administration, and data export gamification (capture the flag (CTF)).
- **Scenario Editor/Builder** – to modify or create new threat scenarios, integrating customer's own VMs or external devices with full flexibility in defining their own network topology, while displaying topology elements in a nice diagram.
- **Tools** – traffic generators (i.e., BreakingPoint), SIEM, exploit tools and frameworks, web servers, firewalls, IDS/IPS and more.
- **Threat scenarios** – a library of predefined threat scenarios, and the ability to create customized scenarios.
- **Event scenarios** – predefined or custom event scenarios specifically targeted for team-based gamification events, such as Capture the Flag.
- **Learning content** – educational and instructional materials on each cyber exercise.
- **Consulting services** – expertise to build the right solution for each organization, including customized threat scenarios and event scenarios, as well as integration of 3rd party, commercial or open-source components.
- **Training services** – training on solution implementation and Keysight tools.

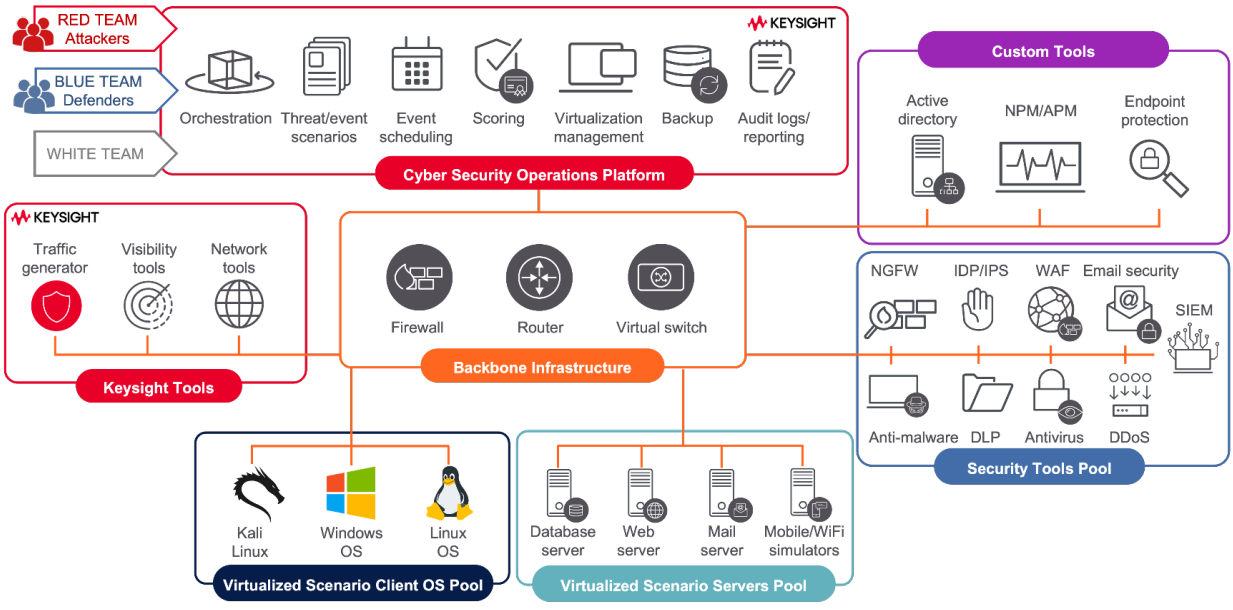


Figure 1. Cyber Security Operations Platform – Solution component architecture.

Key Features

Threat and event scenarios

- Threat and event scenarios simulate networks, traffic, attacks, and defense components to train and test security personnel and expose them to new intervention procedures and technologies in a safe and controllable environment.
- Multi-tenant architecture enables simultaneous users to run out-of-the-box, or custom attack/defense scenarios, using a friendly and intuitive web interface.
- Pre-packaged threat scenarios enable a variety of real user exercises in an isolated and sandboxed environment.
- Advanced threat and event scenario editor for easy customization.
- Step-by-step visual documentation for each pre-packaged scenario.
- Dynamic scenario networking diagram.
- Scenarios mimic an organization's infrastructure enabling realistic attacks and real-time incident response.
- Inventory Editor allows users to modify or create new resource profiles for each VM or Container imported into the platform.
- Scenario Editor lets users modify or create new custom threat scenario within a customized network topology according to each customer's needs.
- Continuously expanding the scenarios library (currently, over 100 scenarios) to provide cutting-edge training and simulation experiences.
- Includes various scenario types, covering tactics (e.g. *"Phishing"*, *"Privilege Escalation"*, *"Persistence"*), techniques (e.g. *"Wi-Fi Injection"*, *"APT"*, *"SQL Injection"*) or NICE NIST framework skills for specific skills or work roles (e.g. *50001*, *S0203*).
- All scenarios are mapped to the NICE NIST framework.
- Certificate of Completion feature to create and grant proof of participation and finalization of specific Threat Scenarios.

Gamification

- Multi-tenant architecture enables multiple teams to compete, by scoring the most points in an allotted time, in a user-collaborative event.
- Creation and management of gaming events including team management, scheduling and event publication control.
- Event reporting (scoring dashboard, and flag journal).
- In-chat feature enables real-time communications during events.
- User profile, history and reporting, group management.

Framework

- Simple update mechanism for the framework, and Virtual Routing Forwarding (VRF) components. The framework automatically includes VRF component for update.
- Intuitive web interface with same look-and-feel for different permission-level users. The Framework incorporates role-based access control.
- Transparent environment deployment and orchestration.
- Custom VLAN editor for separating and naming customer logical network segments.

- Built-in isolation mechanisms to prevent interference between different tenants.
- Continuous resource monitoring (CPU, RAM, Disk) across all cluster VMs.
- On-the-fly VM template custom sizing (vCPU and RAM).
- Export event data to external database (for customized post-reporting and historic data retention).
- Easy addition of quiz and flag clues from within the scenario editor.
- Ability to save, export or import groups of virtual machines, and network segments.

Administration

- Admin tools – backup/restore/upgrade.
- Centralized Licensing Manager for Keysight product licenses.
- Secure terminal console + SSH CLI for administrative and network configuration purposes.
- SSL Certificate Manager.
- Centralized logging and diagnostics.
- Lightweight Directory Access Protocol (LDAP) and MeshCentral integration, facilitating remote monitoring and management (RMM) features, and triage and screen recording for instructor-led training.

Capture the Flag

The Capture the Flag event is an extended cybersecurity exercise where multiple teams race against time and each other to find as many “flags” hidden within the virtual infrastructure as possible, scoring points in the process, and demonstrating their skills and knowledge of both offensive and defensive techniques.

The current implementation of Capture the Flag involves purple teaming, where each team of experts assume the role of both red and blue team functions (based loosely on the individual user preference) to deliver a joint approach to the threat they need to mitigate or pose.

Each team is allocated an isolated virtual environment that prevents opposing teams from interfering with each other. Team members collaborate to find as many flags, worth a varying number of points, as possible in the shortest amount of time.

White team users act as supervisors throughout the process, monitoring flag submissions and responding to in-chat requests from the event users. The white team has complete control over the environment and see user and team scores in real-time.

Event scheduling

A white team member (administrator) schedules and configures Events. Users and white team users/administrators can see the scheduled events in advance and have a separate tab to view past events. Administrators can schedule Events directly or save Events as drafts for later modification.

Teams

Each cyber range user can create their own team, within their user profile, using a system-enabled configuration function. Other users can then join a team by issuing a join request from their profile to the team owner.

Each user can select an individual event (or color) preference – such as red, if they prefer an attacking role, or blue if they choose to manage the defense. This helps the White team to establish a suitable attack/defense equilibrium while managing teams.

White team users have complete control over the environment. They can create teams, assign users to teams, delete teams, or change team ownership.

Reporting

The Range or System Administrators can select a static location, either database or network location, to store logs associated with completed events. The completed events location is configured once and will apply to all subsequent events.

Alternately, when scheduling an event, there is an option to enable/disable automatic publication of data after an event is completed (successfully or not). When automatic publication is off, once the event finishes, a white team user can manually publish the event data by clicking on the provided button.

Users can create a detailed customized report of completed events by using the external database export and their own reporting tools.

User Interface

The Range user interface includes an enhanced Scenario editor. The editor enables users to edit a threat scenario with modifications such as removing a quiz or adding event flags with metadata that includes flag type, value, points, points, category, and prefix.

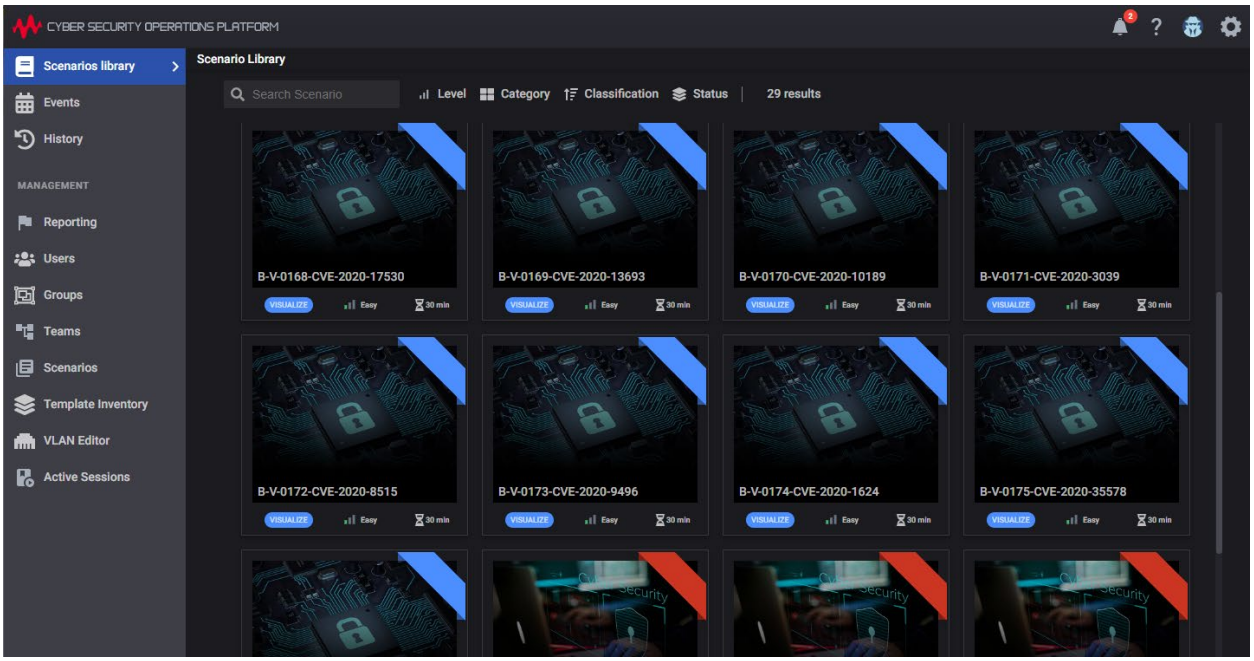


Figure 2. Cyber Security Operations Platform – Scenario library

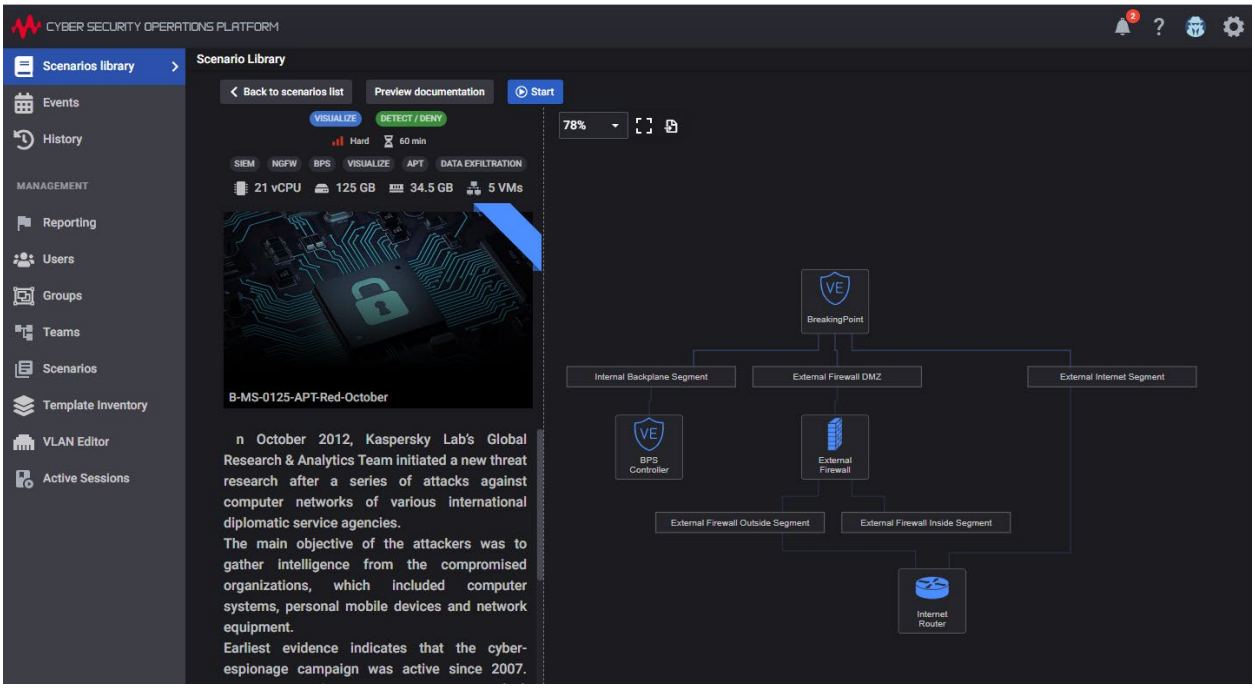


Figure 3. Cyber Security Operations Platform – A threat scenario and associated network diagram

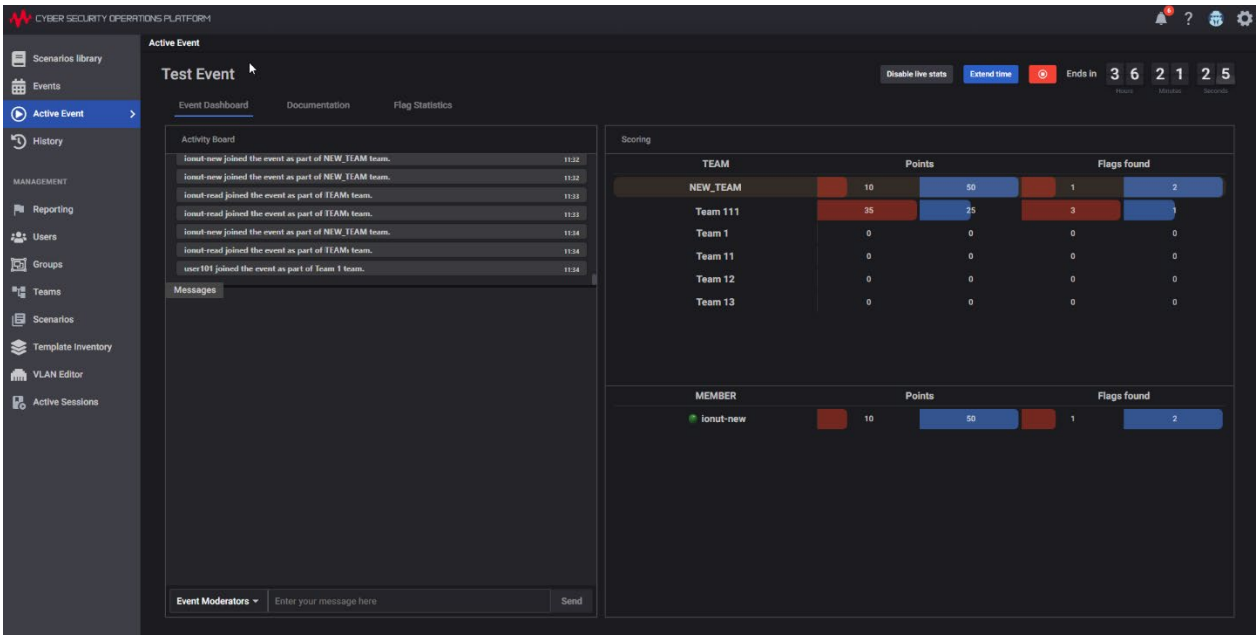


Figure 4. Cyber Security Operations Platform – Active Event main dashboard for a white team user

Figure 5. Cyber Security Operations Platform - Cluster Settings with options to reboot or start VMs directly from the cluster.

Cyber Range Exercises at Work

Role-based training and exercises give users a chance to work together, improving collaboration, communication, and response time during a cyber incident.

Kill Chain stages

The Cyber Kill Chain framework is a theoretical model designed by Lockheed Martin to describe an attack's structure. The sections defined, like links in a physical chain, represent points at which security professionals can detect, arrest, or thwart the attack.

The proposed cyber exercises are based on one or more of the simplified kill chain stages in either the Red Team or Blue Team classification, depending on the threat scenario objectives. Red Team focuses on attacks and understanding the Techniques, Tactics and Procedures (TTPs) used to breach defenses and evade common defense mechanisms. Blue Team specializes in defense and focuses on threat mitigation and visibility.

Keysight advocates that the teams work together to develop better defense strategies and implementation. This results in a deep appreciation and understanding of the reason certain controls are in place, as well as the techniques actively used to circumvent them.

Table 1. Red Team and Blue Team Functions in Kill Chain Stages

Red team		Blue team	
Kill Chain stage	**Simplified stage**	**Kill Chain stage**	**Simplified stage**
Reconnaissance	Reconnaissance	**Protect**	Visualize
Weaponization	Exploitation	**Detect**	Protect
Delivery		**Deny**	
Exploitation		**Disrupt**	
Command + Control	Persist	**Contain**	Contain
Objective / Target		**Recover**	

Each threat scenario is mapped to NICE NIST framework (SP 800-181, version 2 currently in draft). The NICE Workforce Framework for Cybersecurity, commonly referred to as the NICE Framework, is a nationally focused resource to help employers develop their cybersecurity workforce. It establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed. The NICE Framework applies across public, private, and academic sectors.

Hardware Requirements

Keysight's Cyber Security Operations Platform consists of the following components:

- **CySOP VM image** – virtual machine that runs the Cyber Security Operations Platform's main services and web interface.
- **CySOP VRF image** – virtual machine that facilitates Virtual Routing Forwarding connectivity from the User Network into the cyber range.
- **CySOP Global Web Server** – virtual machine hosted on a shared segment that contains configurations and scripts used in the threat scenarios.
- **Scenario's VM Templates** – fully pre-configured operating system image, used to deploy virtual machines/containers. A users will deploy the appropriate VMs in an automatic way each time a Threat Scenario is started; when the scenario stops, the associated VMs will be destroyed, and resources will be released back to the hypervisor.[1]

The outline below shows platform component requirements that satisfy the base system but do not cover the pre-defined or custom threat scenario requirements.

	CySOP VM	CySOP VRF	CySOP Global Web Server	Scenarios' Templates	Template Sync Tool
vCPU	8 vCPUs	2 vCPUs	1 vCPU	Depending on the number of tenants	1 vCPU
Memory	16 GB RAM	2 GB RAM	1 GB RAM		0.5 GB RAM
Disk	120 GB	32 GB	20 GB	Min. 3 TB	1 GB

[1] Currently our VM templates require ~3 TB of disk space; high-performance disks will have a direct impact on the execution when it comes to the speed to start and orchestrate the VMs. Therefore, we recommend using PCIe Gen 4x4 Non-Volatile Memory Express (NVMe) SSD disks or higher, wherever possible.

Ordering Information

P/N	Description
Subscription licenses	
983-4101[1]	TAA Compliant, Cyber Security Operations Platform (CySOP) Promotional Bundle – w/10 tenants, Subscription License (1-year), FLOATING (983-4101) Includes: • licensing to support the execution of user administration, learning, orchestration, threat scenarios and Capture the Flag (CTF) within a cyber range solution. • 10 tenants per deployment • the first year of maintenance and support • qty = 1 x BreakingPoint Virtual Edition (VE) - 1GE 1-year Subscription License (939-9600) Does not include services, traffic generation tools, or network components (purchased separately)
983-4102	TAA Compliant, Cyber Security Operations Platform (CySOP) Promotion optional add-on to add five additional tenants, Subscription License (1-year), FLOATING (983-4102) Includes: • provides an additional 5 tenants for threat scenarios and capture the flag (CTF) • can be used cumulatively, up to the system supported by a maximum of 120 tenants per installation. Requires: Purchase of 983-4101
972-5911	TAA Compliant, Cyber Security Operations Platform (CySOP) - Subscription License, FLOATING (972-5911) Includes: • licensing to support the execution of user administration, learning, orchestration, and threat scenarios within a cyber range solution. • (List price is per unit, per year) • supports full complement of 120 Tenants. Requires: • License term to be specified in 1-year increments for a maximum of 5-years; Does not include professional services, traffic generation tools, or network components (purchased separately).
972-5912	TAA Compliant, Cyber Security Operations Platform (CySOP) – Capture the Flag Feature - Subscription License, FLOATING (972-5912) Includes: • licensing to enable the operation of the Capture the Flag feature within the Cyber Security Operations Platform (List price is per unit, per year). • supports full complement of 120 Tenants. Requires: • Purchase of 972-5911 • License term to be specified in 1-year increments for a maximum of 5-years Does not include professional services, traffic generation tools, or network components (purchased separately).
Perpetual licenses	
983-4001[2]	TAA Compliant, Cyber Security Operations Platform (CySOP) Promotional Bundle - w/ 10 tenants, Perpetual License, FLOATING (983-4001) Includes: • licensing to support the execution of user administration, learning, orchestration, threat scenarios and Capture the Flag (CTF) within a cyber range solution. • 10 tenants per deployment • the first year of maintenance and support • qty = 1 x BreakingPoint Virtual Edition (VE) - 1GE Perpetual License (939-9609) Does not include services, traffic generation tools, or network components (purchased separately)
983-4002	TAA Compliant, Cyber Security Operations Platform (CySOP) Promotion optional add-on to add five additional tenants, Perpetual License, FLOATING (983-4002). Includes: • provides an additional 5 tenants for threat scenarios and capture the flag (CTF) • can be used cumulatively, up to the system supported by a maximum of 120 tenants per installation. Requires: Purchase of 983-4001

P/N	Description
972-5921	TAA Compliant, Cyber Security Operations Platform (CySOP) - Perpetual License, FLOATING (972-5921) Includes: • licensing to support the execution of user administration, learning, orchestration, and threat scenarios within a cyber range solution. • the first year of maintenance and support. • supports full complement of 120 Tenants. Does not include services, traffic generation tools, or network components (purchased separately).
972-5922	TAA Compliant, Cyber Security Operations Platform (CySOP) - Capture the Flag Feature - Perpetual License, FLOATING (972-5922) Includes: • licensing to enable the operation of the Capture the Flag feature within the Cyber Security Operations Platform. • supports full complement of 120 Tenants. Requires: • Purchase of 972-5921 Does not include professional services, traffic generation tools, or network components (purchased separately).
Perpetual renewals	
909-4101	TAA Compliant, Cyber Security Operations Platform (CySOP), Extended Maintenance Renewal for Perpetual CySOP products • Applies SKUs 972-5921, 972-5922, 972-5971, 983-4001 and 983-4002 • Annual Price is 18% of current Software list price.

1 For 983-4101 – Up to 120 tenants per system are supported. An optional group of 5 tenants can be purchased using (9xx-xxxx 5-tenants add-on). Optionally, additional BreakingPoint Virtual Edition 1GE 1-year Subscription licenses can be ordered using 939-9600.

2 For 983-4001 – Up to 120 tenants per system are supported. An optional group of 5 tenants can be purchased using (9xx-xxxx 5-tenants add-on). Optionally, additional BreakingPoint Virtual Edition 1GE Perpetual licenses can be ordered using 939-9609.