MITIGATE CYBER AND DEVOPS RISK BEFORE, DURING AND AFTER INCIDENTS
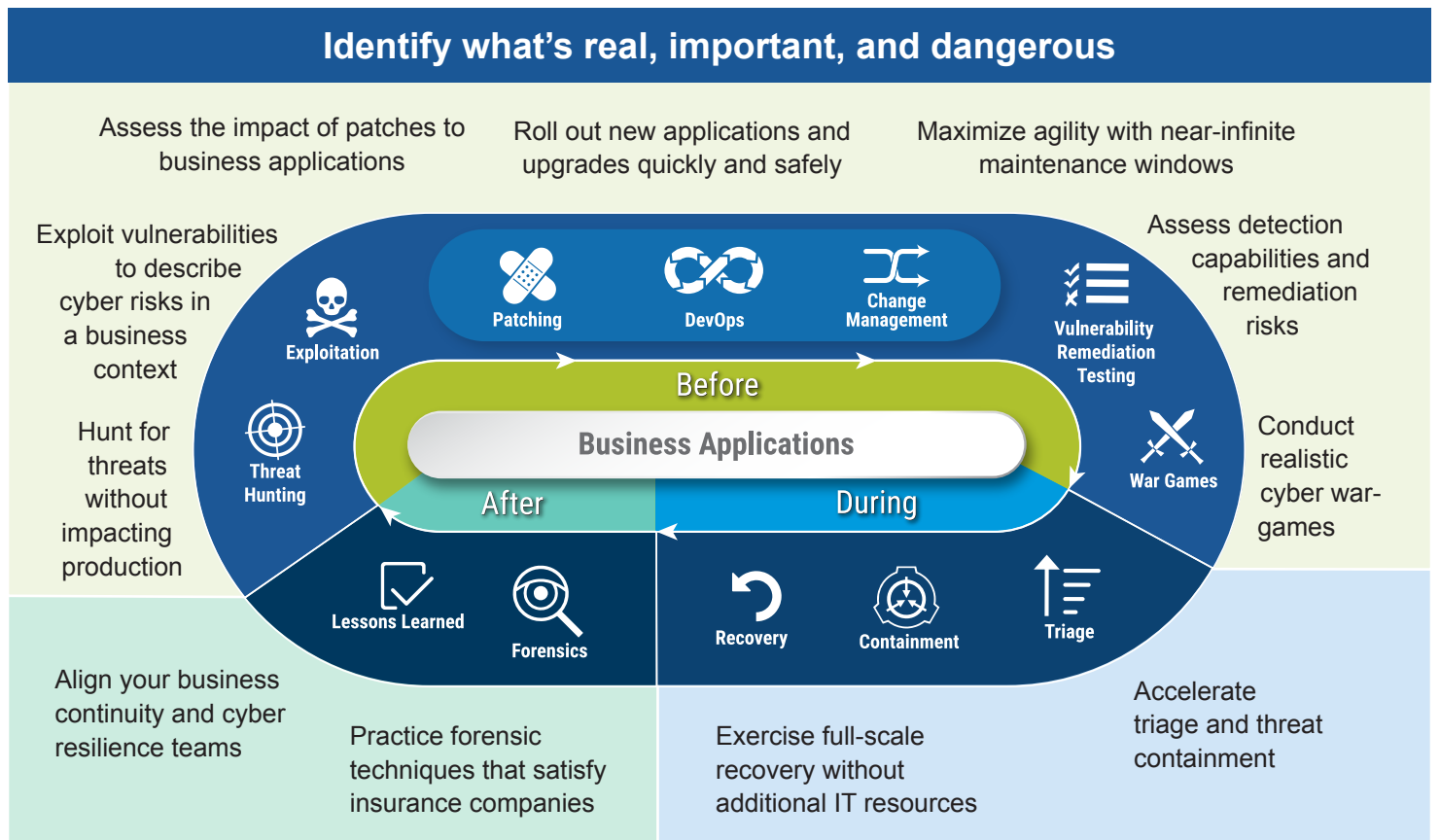
TRANSFORM YOUR DISASTER RECOVERY SITE INTO A VIRTUAL CYBER RANGE

CyberVR™ is a software platform that makes full-scale, extremely realistic, and continuous cybersecurity and DevOps testing possible without affecting production systems, a first in technology risk mitigation.

CyberVR™ creates fully functional copies of production systems in mere minutes without the need for additional infrastructure. Those sandboxes are automatically instrumented and made easily accessible for interactive manipulation by multi-disciplinary teams to optimize workflows, validate change management procedures, and collect evidence of cybersecurity capabilities or weaknesses.
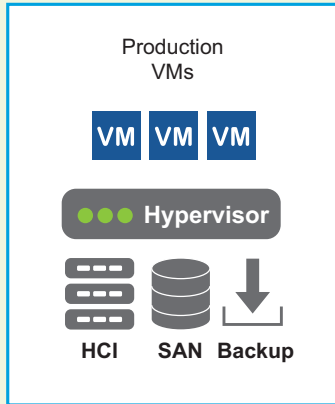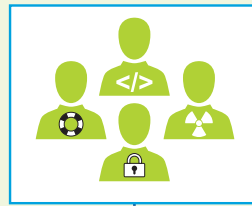
- **Prove** application resilience under destructive cyber attack scenarios
- **Test and validate** risk containment procedures in a realistic sandbox
- **Shorten** cyber vulnerability detection and remediation times
- **Remediate** cybersecurity findings without fear of system downtime
- **Reduce** patch testing and application validation time to just hours
- **Recover** from severe attacks while retaining key evidence for insurance/governance
- **Mitigate** risks created by frequent DevOps software releases

Prove Your Preparedness. Defend Yourself. Increase Your Confidence.

Identify what's real, important, and dangerous

Assess the impact of patches to business applications

Roll out new applications and upgrades quickly and safely

Maximize agility with near-infinite maintenance windows

Exploit vulnerabilities to describe cyber risks in a business context

Hunt for threats without impacting production

Assess detection capabilities and remediation risks

Conduct realistic cyber war-games

Accelerate triage and threat containment

Align your business continuity and cyber resilience teams

Practice forensic techniques that satisfy insurance companies

Exercise full-scale recovery without additional IT resources

Exploitation · Patching · DevOps · Change Management · Vulnerability Remediation Testing · War Games · Threat Hunting · Before · Business Applications · After · During · Lessons Learned · Forensics · Recovery · Containment · Triage

CyberVR™ Functional Diagram

Ease of access for developers, security teams, pen testers

CyberVR™

Production VMs

VM VM VM

●●● Hypervisor

HCI   SAN   Backup

Application landscapes and networks discovered

Bubble Deployment

Functional and isolated Network Bubbles including applicatoins

Efficient Snapshot Clones

Integrated cyber exercises

VM VM VM

●●● Hypervisor

HCI   SAN   Backup

Replicated Snapshots
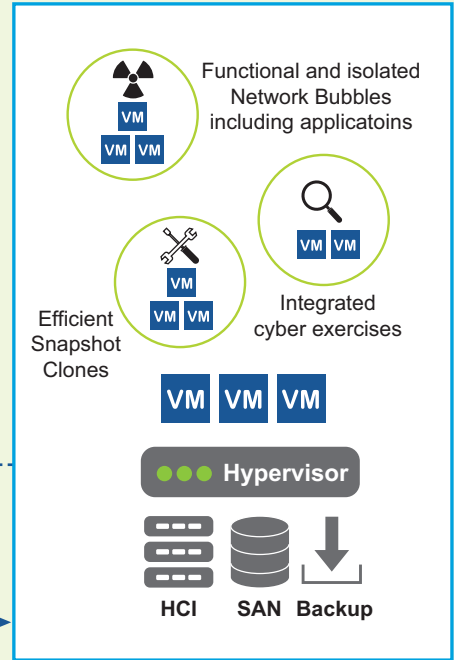
CyberVR™ takes advantage of efficient snapshot clones to automate the creation, instrumentation, and operation of full-scale datacenter sandboxes that are used to safely discover, assess, mitigate, eradicate, and recover from IT corruption and cybersecurity incidents. Now you can prove application resilience, reduce detection and remediation times, anticipate patching side effects, and provide forensic information required for cyber insurance claims.

Key Components of the CyberVR™ Simulation Platform

Feature	Description
Production Workloads	Virtualized production workloads are at the core of CyberVR™: it automatically detects which VMs are protected by snapshots and where those snapshots reside. CyberVR™ then automatically reconstructs the VMs that support a workload and their interconnection fabric so that they can run just as if they were in the production environment.
Tight integration with virtualized infrastructure	With efficient Snapshot Clones, enterprises get near-zero RTOs for VMs and databases. CyberVR™ expands their use to also provision, instrument, and operate multiple clones in fully functional sandbox environments for security, change management, and test/dev without a storage penalty.
Functional Isolated Network Bubble	Restored copies of the production VMs combined with built-in software defined networking capabilities provide fully functional yet isolated networks that are easily configured, instrumented, and operated through CyberVR™. Local snapshots of the VMs are taken during simulations, making possible "what-if" analysis and multi-path drill execution.
Integrated Exercises	Pre-packaged tools and exercises can be automatically applied to any simulation, including but not limited to OpenVAS, Metasploit, MBSA, WSUS, mass credential re-issue, full-scale patch installation and validation, etc. CyberVR™ automatically generates operational and compliance reports and performs user-defined application health checks during simulations.
Participants	Multi-disciplinary teams including developers, security analysts, and application can safely deploy and connect to the isolated networks for testing and training using the CyberVR™ self service portal. Access though the hypervisor is also available for system administrators.

Contact us for a demo or trial and have CyberVR™ up and running in your environment in less than 2 hours