Palo Alto Unit 42 & Google Mandiant ESXi Recommendations

	PALO ALTO UNIT 42	GOOGLE MANDIANT	HOW VALI CYBER CAN HELP
Credential & Access Monitoring	Monitor vpxuser, SSH/SCP usage, and credential extraction attempts.	Restrict SSH/ESXi Shell access; use named accounts with least privilege; avoid root login.	**CLI MFA and AI-Behavioral Detection analyzes credential usage and access and takes action on malicious behavior.**
Tampering Detection	Detect reverse shells, tunneling, unregistered VMs, and admin impersonation.	Monitor for guest-to-guest command execution and hypervisor-level anomalies.	**Tamper Proteciton & Application Allowlisting prevent unauthorized changes.**
File Integrity Monitoring	Track changes to autobackup.bin, config files, and unauthorized VIB installs.	Audit VIBs; detect force installs; avoid "Community Supported"; monitor for hypervisor-level anomalies	**Application Allowlisting & File Access Prevention stop file system modification so attackers can't gain a foothold.**
Process & Threat Hunting	Monitor hidden Python/Perl daemons and unauthorized background processes.	Use YARA scans and memory dumps to detect implants and stealthy persistence.	**AI-Behavioral Detection, Exploit Prevention, and proactive threat intelligence find threats—including novel threats.**
Logging & Telemetry	Ensure logs are forwarded to SIEM; detect tampering of logging services.	Ensure vmsyslogd is active; detect disabling or tampering of logging processes.	**Process-level networking rules and CLI MFA ensure that ESXi hosts have no suspicious network activity.**
Network Isolation	Isolate management interfaces; restrict SSH/ API/vCenter access via firewall rules.	Mandiant does not address this category.	**CLI MFA helps ensure authorized access. Vali Cyber's solution can also run in air-gapped environments.**
Runtime Threat Detection	Use hypervisor-aware tools; integrate with EDR/XDR. (Note: Unit 42 does not offer a Broadcom-certified solution.)	"UNC3944's playbook requires a fundamental shift in defensive strategy, moving from EDR-based threat hunting to proactive, infrastructure-centric defense."—Google (Note: Mandiant does not offer a Broadcom-certified solution.)	**Vali Cyber provides the only Broadcom-certified runtime solution for ESXi.**
Backup & Recovery	Isolate backups; monitor for ransomware targeting snapshots or volumes.	Mandiant does not address this category.	**Automated remediation can restore files instantly.**
Secure Boot & TPM	Unit 42 does not address this category.	Enable Secure Boot; use TPM 2.0; l everage vSphere Trust Authority for key access control.	**Vali Cyber's solution has fine-grained controls and custom-fit ransomware protections.**

https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report
https://unit42.paloaltonetworks.com/cve-2022-22954-vmware-vulnerabilities/
https://cloud.google.com/blog/topics/threat-intelligence/vsphere-active-directory-integration-risks
https://thehackernews.com/2025/07/scattered-spider-hijacks-vmware-esxi-to.html

valicyber™