










HARDENING, MITIGATION, AND REMEDIATION GUIDES

Mandiant published these guides as white papers or blog content to assist our customers with detection, remediation, and best practices for hardening your systems against attacks. While each can be found on <https://mandiant.com>, we've centralized them here in the documentation portal for easy reference.

- [CVE-2022-30190 - MSDT Mitigation and Detection Recommendations](https://dyzz9obi78pm5.cloudfront.net/app/image/id/6455508e0508e46bd84c6aab/n/cve-2022-30190-msdt-mitigation-and-detection-recommendations.pdf) 
(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/6455508e0508e46bd84c6aab/n/cve-2022-30190-msdt-mitigation-and-detection-recommendations.pdf>)
- [DDoS Protection Recommendations](https://dyzz9obi78pm5.cloudfront.net/app/image/id/6455508fe5f72a58d83e9cac/n/ddos-protection-recommendations-v10.pdf) 
(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/6455508fe5f72a58d83e9cac/n/ddos-protection-recommendations-v10.pdf>)
- [Incident Remediation Recommendations - ESXi and vCenter](https://dyzz9obi78pm5.cloudfront.net/app/image/id/6455508b64ab775417716055/n/incident-remediation-recommendations-esxi-and-vcenter-v10.pdf) 
(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/6455508b64ab775417716055/n/incident-remediation-recommendations-esxi-and-vcenter-v10.pdf>)
- [Linux Endpoint Hardening to Protect Against Malware and Destructive Attacks](https://dyzz9obi78pm5.cloudfront.net/app/image/id/645550913bffdf42eb128b51/n/linux-endpoint-hardening-to-protect-against-malware-and-destructive-attacks.pdf) 
(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/645550913bffdf42eb128b51/n/linux-endpoint-hardening-to-protect-against-malware-and-destructive-attacks.pdf>)
- [Log4Shell - Log4j2 Mitigation Recommendations](https://dyzz9obi78pm5.cloudfront.net/app/image/id/6455508ce5f72a58d83e9cab/n/log4shell-log4j2-mitigation-recommendations.pdf) 
(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/6455508ce5f72a58d83e9cab/n/log4shell-log4j2-mitigation-recommendations.pdf>)
- [Okta Prioritized Hardening and Hunting Recommendations](https://dyzz9obi78pm5.cloudfront.net/app/image/id/645550900508e46bd84c6aac/n/okta-prioritized-hardening-and-hunting-recommendations.pdf) 
(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/645550900508e46bd84c6aac/n/okta-prioritized-hardening-and-hunting-recommendations.pdf>)
- [Proactive Preparation and Hardening to Protect Against Destructive Attacks](https://dyzz9obi78pm5.cloudfront.net/app/image/id/6455508f132d243564156f4a/n/proactive-preparation-and-hardening-to-protect-against-destructive-attacks-v10-for-publishing.pdf) 
(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/6455508f132d243564156f4a/n/proactive-preparation-and-hardening-to-protect-against-destructive-attacks-v10-for-publishing.pdf>)
- [Ransomware Containment Remediation and Recovery Strategies](https://dyzz9obi78pm5.cloudfront.net/app/image/id/64555090d5bb443c3e35c7ea/n/ransomware-containment-remediation-and-recovery-strategies-draft-v110.pdf) 
(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/64555090d5bb443c3e35c7ea/n/ransomware-containment-remediation-and-recovery-strategies-draft-v110.pdf>)
- [Remediation and Hardening for .NET ViewState Deserialization Vulnerabilities](https://dyzz9obi78pm5.cloudfront.net/app/image/id/6455508c4514240b160f6fdf/n/remediation-and-hardening-for-net-viewstate-deserialization-vulnerabilities-v20.pdf) 
(<https://dyzz9obi78pm5.cloudfront.net/app/image/id/6455508c4514240b160f6fdf/n/remediation-and-hardening-for-net-viewstate-deserialization-vulnerabilities-v20.pdf>)