THREATDOWN™

Ransomware Prevention Checklist

Prevention

□ **Patch early, patch often.** In the past 12 months, ransomware gangs have made extensive use of software vulnerabilities in firewalls to penetrate networks. Organizations should prioritize actively exploited and critical vulnerabilities, and ensure that internet-facing systems are patched with security updates on a regular, scheduled basis.

□ **Monitor EDR 24x7.** Ransomware groups know that they are likely to trigger EDR alerts as they prepare an attack, so they work at night when alerts may not be noticed. Organizations should ensure their EDR is monitored 24x7, using in-house security staff, a managed service provider (MSP), or a service like ThreatDown's Managed Detection & Response.

□ **Remove blind spots.** Attackers will seek out blind spots on a network, such as devices that do not have EDR installed, or devices where the EDR has overly permissive exclusions. Organizations should shut down "shadow IT" devices, ensure that all servers and endpoints are protected by EDR, and audit their security policies regularly to eliminate unnecessary exclusions.

Mitigation

□ **Test backups.** Ransomware gangs know that an organization's last line of defense against encrypting ransomware is its backups, so attackers will try to delete them. Organizations should maintain offline backups that can't be reached if the network is compromised and test backups regularly by attempting to restore critical systems from them.

□ **Assign roles and access.** Staff are often unavailable or hard to reach over weekends and holidays, when attacks are likely to occur. Organizations should maintain a contact list of names, phone numbers and roles that can still be accessed if its computer systems are compromised, and ensure that people providing cover for others have the documentation and access they need.

□ **Make a disaster recovery plan.** A well-practiced disaster recovery plan can be the difference between hours of disruption and weeks of downtime. Organizations should document step-by-step procedures for responding to an attack, rehearse them through tabletop exercises, and ensure the plan is accessible even if critical systems are unavailable.

THREATDOWN™ | threatdown.com | sales@threatdown.com