MANDIANT

REFERENCE GUIDE

A TIERED FRAMEWORK FOR CYBER THREAT LEVELS

In a continuously changing cyber threat landscape, defenders have seemingly limitless workloads. To help defenders focus their cyber security efforts, Mandiant developed a three-prong framework that aligns practical readiness and hardening and operational recommendations to three distinct phases of alarm. As an organization's risk of cyber attacks fluctuates over time, these stages offer tangible operational actions that can be implemented and retracted as needed. The goal of the framework is to help organizations evaluate their security posture in response to their assessed level of risk and perceived threats and vulnerabilities. This framework provides flexibility for organizations to escalate, de-escalate and maintain a steady state of active cyber defense to combat an array of cyber threats.

Phases of this staged approach to active cyber defense include:

- **Stage 1:** Normal State of Defense (NORMAL)
- **Stage 2:** Elevated State of Defense (ELEVATED)
- **Stage 3:** High Alert State of Defense (EMERGENCY)

For each condition, Mandiant created two categories of recommendations to strengthen an organization's cyber defenses in parallel with rising threat conditions. **Readiness and hardening recommendations** focus on proactive and strategic tasks, while **operational recommendations** identify what operational changes can be adopted to increase their security posture within each phase. Recommendations are general guidelines and can serve as operational examples because it is difficult to account for the unique circumstances and capabilities of every organization. In some cases, recommendations may be aspirational. As organizations escalate from one stage to another, readiness and hardening recommendations from lower-threat stages are intended to be prerequisites for higher-threat stages.

Timing to Maintain Posture/ Strategy for Managing Escalation: Cyber attacks are a constant threat in our modern, interconnected world. It is not realistic for organizations to maintain a heightened state of alert for the foreseeable future. Organizations can reference the recommendations below to help identify when a threat has passed and when they can deescalate their cyber security posture. Escalating and deescalating cyber defenses can be efficiently and effectively accomplished if organizations have dedicated cyber defense processes, such as:

- Maintaining direct lines of communication between the Cyber Threat Intelligence (CTI) team and cyber security staff.
- Conducting regular threat hunting based on the latest threats as identified by the CTI team.
  - Rely on the CTI team to flag any new situations of concern as they would as part of their normal operating process, with threats against your industry of interest or peers taking priority.
- Identifying new detection techniques and procedures.
- Validating near-real-time vulnerability and exploit remediation initiatives, processes, and tools are effective.
- Ensuring efforts are in place to automate hunting and alerts.

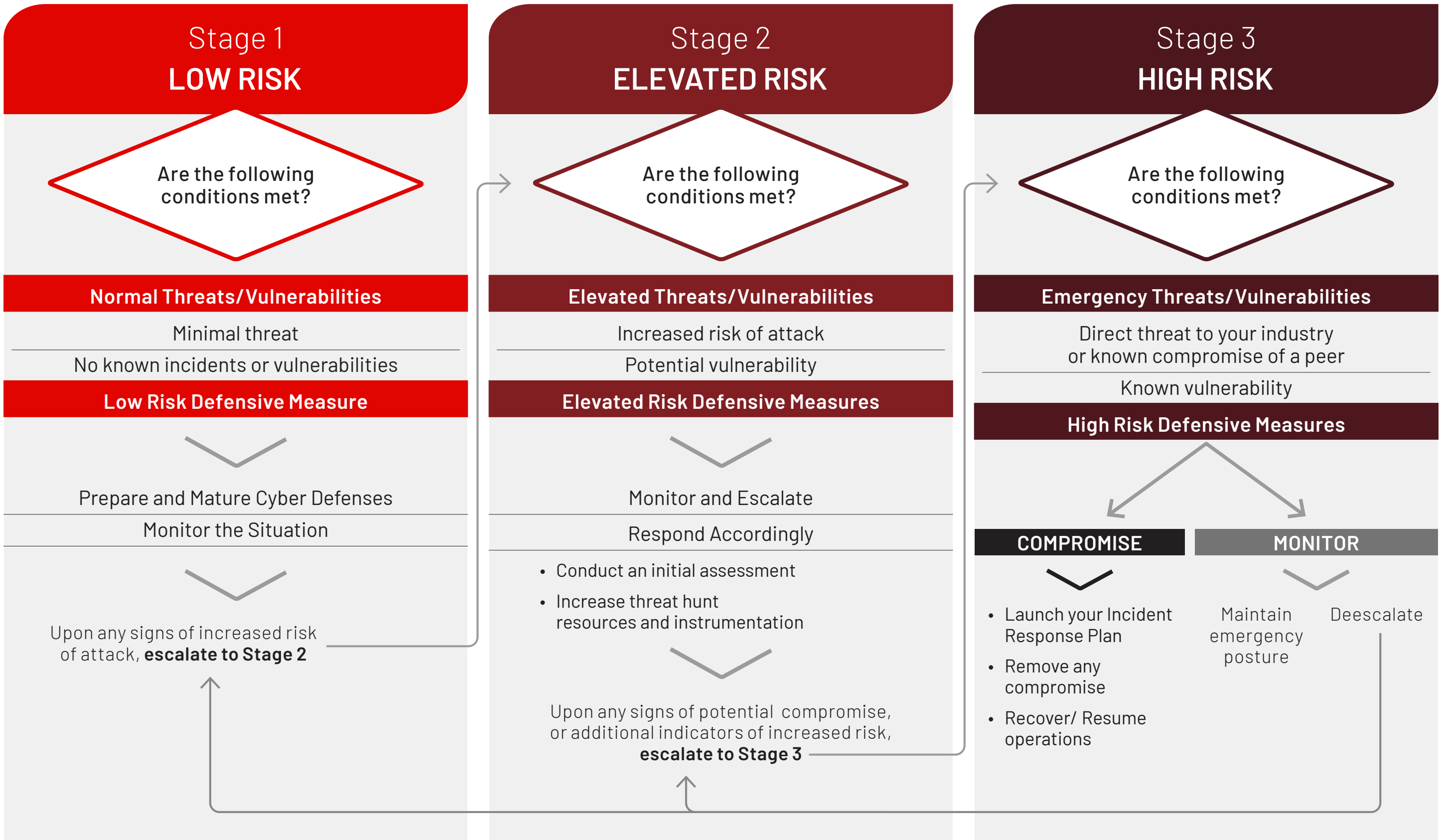
Stage 1
LOW RISK
Are the following conditions met?
Normal Threats/Vulnerabilities
Minimal threat
No known incidents or vulnerabilities
Low Risk Defensive Measure
Prepare and Mature Cyber Defenses
Monitor the Situation
Upon any signs of increased risk of attack, escalate to Stage 2
Stage 2
ELEVATED RISK
Are the following conditions met?
Elevated Threats/Vulnerabilities
Increased risk of attack
Potential vulnerability
Elevated Risk Defensive Measures
Monitor and Escalate
Respond Accordingly
Conduct an initial assessment
Increase threat hunt resources and instrumentation
Upon any signs of potential compromise, or additional indicators of increased risk, escalate to Stage 3
Stage 3
HIGH RISK
Are the following conditions met?
Emergency Threats/Vulnerabilities
Direct threat to your industry or known compromise of a peer
Known vulnerability
High Risk Defensive Measures
COMPROMISE
MONITOR
Launch your Incident Response Plan
Remove any compromise
Recover/ Resume operations
Maintain emergency posture
Deescalate

FIGURE 1. A Tiered Framework for Cyber Threat Levels.

STAGE 1:
Monitor/constant vigilance (NORMAL)

Stage 1 of the Mandiant Tiered Framework for Cyber Threat Levels reflects normal operating procedures when an organization assesses they are at a minimal, or low risk of a cyber attack. These recommendations can help align cyber defenses to best practices and current standards across an organization's environment. Stage 1 can allow organizations to review and proactively protect and harden their security posture. Other recommendations include validating that the existing security posture is applicable to the current threat landscape, and ensuring measures are in place to continuously improve the early detection of cyber threats.

Readiness and Hardening Recommendations

- Visibility, Monitoring, and Orchestration
  - Enable centralized logging for DNS, AD/LDAP/SAML servers, firewalls, cloud platforms and endpoints.
  - Create use case alerts based on industry-specific and organizational threat landscape.
- Identity and Access Management
  - Implement multi-factor authentication (MFA) on all accounts and for externally facing services.
  - Require the use of strong complex passwords.
  - Separate privileged accounts from a user's standard account (such as an account used daily to check emails and access external resources).
- Devices and Endpoints
  - Implement endpoint detection and response tools across the entire environment (on-premises and cloud).
  - Disable macros and harden Microsoft Office and other products.
  - Obtain an inventory of all assets on the domain and network, and have those assets regularly scanned for vulnerabilities.
  - Disable non-essential ports and protocols.
- Networking and Infrastructure
  - Implement network detection and response (NDR) tools for Crown Jewel network zones.
  - Install a web proxy and firewalls to segment and harden external-facing assets and internal network zones.
  - Identify and harden externally facing assets and pathways into the environment.
  - Block common lateral movement ports such as SMB, WMI and WinRM from externally facing or critical systems using host-based firewalls.
  - Ensure backups are performed on a regular basis and are stored separate from network connections.
  - Install an e-mail threat prevention solution.

Operational Recommendations

- Segment information technology (IT) and operational technology (OT) environments.
- Take advantage of partner or third-party capabilities to validate and enhance your security posture.
- Designate a crisis-response team with main points of contact for a suspected cyber security incident and roles/responsibilities within the organization.
- Implement best practices from the Cybersecurity and Infrastructure Security Agency (CISA) and other cyber security organizations and experts. See the below list of references for additional information.
- Test backup procedures to ensure that critical data can be rapidly restored, and critical business functions can remain available in the event of an incident.
- Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.

See the following resources for additional cyber defense best practices:

- Mandiant white paper "Proactive Preparation and Hardening to Protect Against Destructive Attacks"
- CISA Shields Up guidance
- CISA Cybersecurity Best Practices
- CISA Sharing Cyber Event Information guidance
- Amazon AWS Security best practices
- Microsoft Azure Security best practices
- Google Cloud Security Best Practices
- IT security standards

STAGE 2:
Escalate if/when you're at a higher risk (ELEVATED)

When an organization assesses they are at an increased risk of destructive or disruptive cyber attacks, Stage 2 of the Mandiant Tiered Framework for Cyber Threat Levels provides recommendations for assuming a defensive readiness posture. The goal of Stage 2 is to assist with preparing for an attack in a methodological manner. In this phase, defensive actions are prioritized over the potential impact to business operations. When deescalating from this phase, organizations may reverse some restrictive actions while leaving others permanently in place. Recommendations in this phase are meant to disable the depth of access an adversary needs to leverage to achieve their mission. Additionally, increasing threat hunting operations can provide confidence that an adversary does not maintain access to the organization's network and infrastructure. Cyber defense strategies implemented in Stage 2 aim to increase an organization's security posture at a sustainable cadence that can be maintained over many months or for years.

Readiness and Hardening Recommendations

- Visibility, Monitoring, and Orchestration
  - Create use cases and alerts for current and imminent threats based on intelligence.
  - Conduct specific tabletop exercises that are aligned to the current threat landscape.
  - Work with ISACs to obtain and contribute industry-related intelligence.
- Identity and Access Management
  - Request that all privileged account holders reset passwords every month.
  - Increase the use of multi-factor authentication (MFA), if it is not already in place.
  - Review and validate MFA methods and associated devices, ensuring that only authorized and approved devices are registered and enforced for accounts.
  - Terminate all active connections on a regular basis and reset connection states. This applies to authentication sessions as well as remote access connections.
  - Ensure the built-in local administrative account on endpoints is being randomized and automatically rotated (e.g., Microsoft LAPS or other PAM solutions).
  - Understand how to tune your authentication system to decrease risk. For example:
    - Reduce the time for password or authentication caching.
    - Increase the frequency of password rotation for all accounts.
  - Create guardrails and authentication silos for privileged accounts (such as restrict remote authentication).
- Devices and Endpoints
  - Create boundaries and tiers for systems based on criticality to the environment and organization (such as Tier 0, Tier 1, Tier 2).
  - Disable unused and unnecessary services and shares on externally facing and critical assets.
  - Increase data security controls on mobile devices.
  - Use application whitelisting on externally facing and critical systems.
- Networks and Infrastructure
  - Require use of encrypted email communications.
  - Restrict egress communications on critical systems.
  - Apply geo-location blocking based on threat intelligence.

Operational Recommendations

- Send Cyber Security best practices reminders.
- Conduct ad-hoc penetration testing exercises on all externally facing assets.
- Identify contingency resources (funds, people) and ensure they are available.
- Test the Incident Response Team's reaction times.
- Increase the sensitivity of your alert structure.
- Reduce integrations with external services.

STAGE 3:
Highest level of attention (EMERGENCY)

When an organization assesses they are at risk for an imminent, active, or significant cyber attack, Stage 3 of the Mandiant Tiered Framework for Cyber Threat Levels provides recommendations to help thwart, detect, degrade, and remove an adversary's access to your network and infrastructure. An example event that can warrant escalation to Stage 3 may involve an attack targeting near-peer organizations, industries or infrastructure and cyber threat intelligence indicating your organization is at high-risk. Measures executed during this phase may be deemed short-term protections - as they could be disruptive to an organization's business.

Readiness and Hardening Recommendations

- Visibility, Monitoring, and Orchestration
  - Conduct regularly scheduled threat hunts around specific threats that may be in the network.
- Identity and Access Management
  - Increased frequency of password rotation for administrative accounts to daily and rotate passwords for standard accounts every week.
  - Create additional tiering of identities based on the criticality of assets (such as Tier 0 – Privileged Accounts, Tier 1 – Privileged Accounts, Tier 2 – Standard Accounts, etc.).
  - Terminate all active connections daily and reset connection states. This applies to authentication sessions as well as remote access connections.
  - Restrict the scope of accounts that can remotely access and interface with systems (such as Network Logon, Interactive, Terminal Services, Services, Batch Logon).
- Devices and Endpoints
  - Utilize Privileged Access Workstations (PAWs) for performing all administrative tasks.
  - Disable or block built-in tools that can be abused such as PowerShell and PSExec.
  - Block removable devices from being used on endpoints.
  - Use application whitelisting across all endpoints in the environment.
- Networks and Infrastructure
  - Restrict communications between endpoints. Force all internal business-related transactions. through monitored services.
  - Restrict the ability of identities to traverse across different asset tiers (such as Tier 1 identities not able to login to Tier 2 assets).

Operational Recommendations

- Focus on critical asset protection.
  - Protect specific high-value infrastructure and prepare for recovery from a destructive attack.
    - Back up critical assets.
    - Protect virtualization infrastructure.
    - Reset virtual machines (VMs) to a certain or known good state on a periodic basis.
- Shift resources from penetration testing to threat hunting.
- Change network architecture to limit or remove adversary access to critical systems.
  - Restrict remote access.
  - Require full-tunnel VPN connections.
  - Create a secondary Administrative VPN profile for Administrators to access the environment.
  - Where possible, isolate or disconnect compromised or crown jewel systems.
- Update gold images and apply to all high value assets in the organization.
- Conduct continuous compromise assessments of your environment.

If a compromise is detected at this stage, implement your organization's Incident Response plan to contain and remediate the attack.

- See CISA Federal Government Cybersecurity Incident and Vulnerability Response Playbooks, which provides federal civilian executive branch (FCEB) agencies with operational procedures for planning and conducting cybersecurity incident and vulnerability response activities.

Learn more at **www.mandiant.com**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT