2.5 Assignment: Using KPIs

1. Provide the name of the Security KPI and a clickable link that opens in a new tab.

1. Level of Preparedness
Link: Tunggal, A. T. (2023, May 22). *14 Cybersecurity Metrics + KPIs to Track*. UpGuard. https://www.upguard.com/blog/cybersecurity-metrics

2. Non-human Traffic (Bad Bot / Automated Traffic Rate)
Link: Group, T. (2025, April 15). *Artificial Intelligence Drives Surge in Bot Traffic, Now Surpassing Human Activity, According to 2025 Imperva Bad Bot Report*. Thales Cloud Security Products; Thales Group. https://cpl.thalesgroup.com/about-us/newsroom/2025-imperva-bad-bot-report-ai-internet-traffic

3. Mean Time to Detect (MTTD)
Link: *Top CISO Cybersecurity and Cloud Security Metrics | BitSight*. (2020). Bitsight. https://www.bitsight.com/blog/the-most-useful-and-impactful-security-metrics-every-ciso-should-have

4. Mean Time to Acknowledge (MTTA)
Link: Atlassian. (2021). *MTBF, MTTR, MTTF, MTTA: Understanding incident metrics*. Atlassian. https://www.atlassian.com/incident-management/kpis/common-metrics

5. Patching Cadence (Time-to-Patch for High-Risk Vulnerabilities)
Link: Cybersecurity and Infrastructure Security Agency. (2023). *Known Exploited Vulnerabilities Catalog | CISA*. Www.cisa.gov. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

6. Multi-Factor Authentication (MFA) Coverage Rate
Link: CISA. (n.d.). *Turn on Multi-Factor Authentication (MFA)*. CISA. https://www.cisa.gov/secure-our-world/turn-mfa

7. False Positive Rate (FPR) for Security Alerts
Link: *SOC Metrics: Security Metrics & KPIs for Measuring SOC Performance*. Splunk. https://www.splunk.com/en_us/blog/learn/security-operations-metrics.html

8. Security Logging / Telemetry Coverage (SIEM / EDR Visibility)
Link: NIST. (2025). *Cybersecurity Framework*. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

9. Backup Restore Success Rate (Recovery Testing Pass Rate)
Link: CISA. (2023). *Stop Ransomware*. Www.cisa.gov. https://www.cisa.gov/stopransomware

10. Phishing Susceptibility Rate (Click / Credential Submission Rate)
Link: CISA. (n.d.). *Recognize and Report Phishing | CISA*. Www.cisa.gov. https://www.cisa.gov/secure-our-world/recognize-and-report-phishing

2. Using a minimum of 25 words for each, explain the KPI and how it is used in a real-world situation.

KPIs
Five that were discussed this week.
1. Level of Preparedness

Explanation: Level of preparedness is effectively a "how ready are we?" KPI that measures whether or not an organization has people, process, and tooling in place prior to something breaking. In a live environment, I would track preparedness with leading indicators such as % of critical systems covered by monitoring, % of incident response playbooks tested in tabletop exercises, and team response time to execute containment steps. This KPI matters to me because it helps eliminate panic during incidents and increase repeatability of response.

2. Non-human Traffic (Bad Bot / Automated Traffic Rate)

Explanation: Non-human traffic tracks the percentage of all inbound web/app/API traffic that is bot traffic instead of from real customers. Security operations teams measure this KPI in the physical world to gain context on abuse (credential stuffing, scraping, card testing) and tune WAF/bot management controls accordingly. A spike in non-human traffic rate is an indicator to hunt for automation attacks, change rate limits, add bot challenges, or tighten API auth to secure uptime and customer data.

3. Mean Time to Detect (MTTD)
Explanation: MTTD is a measurement of the time duration that threats and incidents remain undetected. In practical terms, SOC teams often use MTTD as a measure of monitoring and detection engineering effectiveness. After all, you can't contain what you don't detect. If your MTTD is trending downward over time, that typically means you have better telemetry, better correlation rules, and better triage. If it is trending up, you can end up with alert fatigue, missed log sources, or blind spots which put your organization at greater risk.

4. Mean Time to Acknowledge (MTTA)
Explanation: MTTA measures the amount of time it takes for an organization to begin working an alert, from the time the alert is received. In real-world operations, MTTA is a way to indicate whether alerting and on-call coverage is practical, and whether the SOC has the right staffing and is empowered to respond. In my opinion, MTTA is particularly valuable for understanding “process friction” such as noisy alerts, unclear escalation paths, or missing runbooks, which can slow down first response.

5. Patching Cadence (Time-to-Patch for High-Risk Vulnerabilities)
Explanation: Patching cadence is the rate at which an organization deploys security patches or mitigations for vulnerabilities classified as high risk after release. In practice, the KPI is leveraged by vulnerability management (VM) and IT operations (IT Ops) to monitor the amount of time assets are exposed to known vulnerabilities that are actively being exploited in the wild. Effective cadence shortens the amount of time where an organization is susceptible to threat actors exploiting technical details published with the vulnerability disclosure. Ineffective cadence is more likely to correlate with higher risk exposure, additional compensating controls, and emergency patching under pressure in the future.

Five that were not discussed this week.
6. Multi-Factor Authentication (MFA) Coverage Rate
Explanation: MFA coverage rate is the percentage of accounts (typically privileged and remote-access accounts) that are covered by MFA. This is a real-world KPI used to prevent credential-based breaches, since a stolen password alone should not be sufficient to log in. I would track MFA coverage rate separately for admins, VPN/SSO, and high-risk apps. Low MFA coverage enables leadership to prioritize rollouts, mandate conditional access, and eliminate exceptions.

7. False Positive Rate (FPR) for Security Alerts
Explanation: False Positive Rate (FPR) is a measure of the amount of security alerts that are investigated, and then ruled as benign activity and not a real threat. In an actual SOC, a high FPR means wasting analyst time, causing alert fatigue, and delaying or distracting from true incidents. Monitoring FPR can allow teams to tune detection rules, improve correlation, and focus on higher-fidelity signals so the team is focused on the things that actually matter.

8. Security Logging / Telemetry Coverage (SIEM / EDR Visibility)
Explanation: Logging/telemetry coverage tracks how much of the organization's critical assets are generating actionable security logs to a central location (SIEM) and/or have EDR agents deployed. This KPI really matters in the real world because without visibility, detection and investigations are impossible. Low coverage could explain high MTTD and poor incident reconstruction, but it also provides a simple, actionable target: onboard missing systems, standardizing log retention.

9. Backup Restore Success Rate (Recovery Testing Pass Rate)
Explanation: This KPI measures the ability to restore backups successfully and within the planned recovery time objective (RTO) and recovery point objective (RPO). It's not uncommon in real-world ransomware incidents for the organization to find out too late in the game that backups are missing or restores don't work. Monitoring restore success rate enforces regular testing, confirms that critical systems are actually recoverable, and offers evidence to leadership that investments in resilience are paying off.

10. Phishing Susceptibility Rate (Click / Credential Submission Rate)
Explanation: The Phishing susceptibility rate is a KPI which shows how frequently a user will click a phishing link, open a malicious attachment, or provide credentials during a phishing simulation (and sometimes real reported phishing trends). Phishing Susceptibility rate in the real world is often used as a measure of security awareness

effectiveness, or as a way to pinpoint high-risk departments for tailored security training. I like this KPI because it is quantitative and it can show improvement when coupled with a more mature reporting culture and safe email controls.

3. Research current events and case studies and provide a real-world example that demonstrates how a KPI was utilized or how it could have been utilized to combat the situation in the example. Be sure to include a clickable link.

1. Level of Preparedness
Event: In September 2025, CISA warned about a widespread software supply chain compromise affecting the npm ecosystem. Link: *Widespread Supply Chain Compromise Impacting npm Ecosystem | CISA*. (2025, September 23). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem

- How the KPI was utilized / could have been utilized to combat the situation: If an organization measures preparedness (dependency governance, code-scanning coverage, SBOM adoption, incident playbooks for compromised packages), then they can respond faster. That means identifying where vulnerable packages exist, quarantining builds and rotating secrets as needed, and quickly communicating impact clearly. Preparedness also involves a repeatable process for emergency dependency pinning as well as verification of pre-production deployment to reduce blast radius.

2. Non-human Traffic (Bad Bot / Automated Traffic Rate)
Event: The 2025 Imperva Bad Bot Report noted automated traffic surpassed human traffic and highlighted AI-driven bots as a major trend. Link: Group, T. (2025, April 15). *Artificial Intelligence Drives Surge in Bot Traffic, Now Surpassing Human Activity, According to 2025 Imperva Bad Bot Report*. Thales Cloud Security Products; Thales Group. https://cpl.thalesgroup.com/about-us/newsroom/2025-imperva-bad-bot-report-ai-internet-traffic

- How the KPI was utilized / could have been utilized to combat the situation: If an organization is tracking non-human traffic KPI by endpoint and geography, abuse patterns such as credential stuffing and scraping will be found. That KPI can inform actions such as rate limits, bot challenges, more robust API authentication, fraud controls. Without measurement, leaders may only see performance problems and not the automated attack beneath.

3. Mean Time to Detect (MTTD)
Event: Reuters reported a major breach at Coupang where unauthorized access began in June 2025, but the company discovered it in November 2025. Link: Jin, H., & Lee, J. (2025, December 1). South Korean police probe massive data leak at Coupang. *Reuters*. https://www.reuters.com/sustainability/boards-policy-regulation/south-korean-police-probe-massive-data-leak-coupang-2025-12-01/

- How the KPI was used / could have been used to help with the situation: This is where MTTD comes into play. If Coupang was tracking MTTD and looking to improve it, they could have invested in better anomaly detection for critical use, data access patterns and anomalous traffic. A lower MTTD would have meant less exposure time, a smaller window of accessed data and a smaller scope/cost for the investigation.

4. Mean Time to Acknowledge (MTTA)
Event: CISA and partners released an updated advisory on Akira ransomware in November 2025, showing the threat remains active and evolving. Link: *CISA and Partners Release Advisory Update on Akira Ransomware | CISA*. (2025, November 13). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/alerts/2025/11/13/cisa-and-partners-release-advisory-update-akira-ransomware

- How the KPI was utilized / could have been utilized to combat the situation: In a ransomware attack, seconds count. Monitoring MTTA can be used to demonstrate whether alerts are being triaged in a timely manner and whether on-call coverage matches the reality. If MTTA is high, an organization can tune down alert noise, optimize runbooks and paging, and take steps to ensure the first responder gets containment started sooner before the attack has a chance to spread.

5. Patching Cadence (Time-to-Patch for High-Risk Vulnerabilities)

Event: CISA's Known Exploited Vulnerabilities (KEV) Catalog highlights vulnerabilities confirmed to be used in real attacks. Link: Cybersecurity and Infrastructure Security Agency. (2023). *Known Exploited Vulnerabilities Catalog | CISA*. Www.cisa.gov. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- How the KPI was utilized / could have been utilized to combat the situation: Patching cadence should focus on KEV entries as they are indicative of active exploitation. Tracking the time-to-patch for KEV vulnerabilities allows the leadership to have a clear window of exposure and will enable emergency maintenance approval. If a patch must be deferred, this KPI can be used to also document compensating controls and risk acceptance with timelines.

6. Multi-Factor Authentication (MFA) Coverage Rate

Event: A legal analysis of the Change Healthcare breach describes attackers gaining access via compromised credentials on a remote access portal that lacked multi-factor authentication. Link: Parikh, H., Nighan, M., Montague, V., Mambwe Mutanuka, & Yang, A. (2025, November 12). *The Change Healthcare cybersecurity breach: Impact on healthcare providers*. Nixon Peabody LLP; Nixon Peabody. https://www.nixonpeabody.com/insights/alerts/2025/11/12/change-healthcare-cybersecurity-breach-impact-on-healthcare-providers

- How the KPI was utilized / could have been utilized to combat the situation: If MFA coverage is a KPI that is tracked—particularly for remote access and admins—the business can quickly root out and shut down risky MFA exceptions before they are misused. In my view, MFA coverage is one of the most actionable KPIs, because bolstering it is completely within your control and it significantly lowers the success rate of password compromises and phishing-based logins.

7. False Positive Rate (FPR) for Security Alerts

Event: The 2025 Unit 42 Global Incident Response Report notes that in many incidents, anomalous behavior was flagged but not acted on due to alert fatigue, unclear ownership, or skill gaps. Link: Palo Alto Networks Unit 42. (2025, July 30). 2025 Unit 42 Global Incident Response Report. *Unit 42*. https://unit42.paloaltonetworks.com/2025-unit-42-global-incident-response-report-social-engineering-edition/

- How the KPI was utilized / could have been utilized to combat the situation: If an organization tracks FPR and sees it trending high, it signals the SOC is drowning in noise. Reducing false positives through rule tuning, better correlation, and clearer alert ownership improves the signal-to-noise ratio. That directly supports faster escalation of real suspicious activity and reduces the chance that early warnings are ignored or missed because analysts are overwhelmed.

8. Security Logging / Telemetry Coverage (SIEM / EDR Visibility)

Event: Reuters reported U.S. and Canadian agencies warned about malware used for long-term access and credential theft in targeted systems. Link: Vicens, A. J. (2025, December 4). Chinese-linked hackers use back door for potential "sabotage," US and Canada say. *Reuters*. https://www.reuters.com/world/china/chinese-linked-hackers-use-back-door-potential-sabotage-us-canada-say-2025-12-04/

- How the KPI was utilized / could have been utilized to combat the situation: Lack of long-term visibility makes stealthy access harder to detect. Telemetry gaps: If an organization measures logging/EDR coverage for critical assets, it can reduce gaps in visibility and improve the quality of incident investigations. Better coverage enables faster detection of suspicious authentication, privilege alteration, and lateral movement activities, improving MTTD and response quality.

9. Backup Restore Success Rate (Recovery Testing Pass Rate)

Event: CISA's StopRansomware resources emphasize resilience practices like backups and recovery planning as core defenses. Link: CISA. (2023). *Stop Ransomware*. Www.cisa.gov. https://www.cisa.gov/stopransomware

- How the KPI was used / could have been used to fight back against the situation: A restore success KPI makes "we have backups" defensible proof. Failures or outages over RTO/RPO communicate to leadership that the organization is not truly resilient. This KPI forces routine restore exercises, immutable/offline backups, documented recovery processes so the business can recover quicker and stop paying ransoms.

10. Phishing Susceptibility Rate (Click / Credential Submission Rate)

Event: TechRadar reported a breach at the French Football Federation involving a compromised account used to access administrative software, with phishing being a likely path. Link: Sead Fadilpašić. (2025, December). *Millions of footballers see info leaked after French Football Federation suffers data breach*. TechRadar. https://www.techradar.com/pro/security/french-football-federation-suffers-data-breach-that-compromised-club-members-data

- How the KPI was used / could have been used to address the situation: Phishing susceptibility can be measured to demonstrate if users are still clicking on realistic phishing lures, and to determine if email security controls and user training are working. If this KPI does not go down, the organization can segment higher-risk roles for phishing-resistant MFA, stronger email authentication (DMARC), and tighter restrictions on access to admin tools to reduce the damage from a compromised account.

References (Clickable Links)

• *The Most Important Security Metrics to Maintain Compliance | UpGuard*. (n.d.). Www.upguard.com. https://www.upguard.com/blog/security-metrics

• *Top CISO Cybersecurity and Cloud Security Metrics | BitSight*. (2020). Bitsight. https://www.bitsight.com/blog/the-most-useful-and-impactful-security-metrics-every-ciso-should-have

• Atlassian. (2021). *MTBF, MTTR, MTTF, MTTA: Understanding incident metrics*. Atlassian. https://www.atlassian.com/incident-management/kpis/common-metrics

• Cybersecurity and Infrastructure Security Agency. (2023). *Known Exploited Vulnerabilities Catalog | CISA*. Www.cisa.gov. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

• *Widespread Supply Chain Compromise Impacting npm Ecosystem | CISA*. (2025, September 23). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem

• Group, T. (2025, April 15). *Artificial Intelligence Drives Surge in Bot Traffic, Now Surpassing Human Activity, According to 2025 Imperva Bad Bot Report*. Thales Cloud Security Products; Thales Group. https://cpl.thalesgroup.com/about-us/newsroom/2025-imperva-bad-bot-report-ai-internet-traffic

• Jin, H., & Lee, J. (2025, December 1). South Korean police probe massive data leak at Coupang. *Reuters*. https://www.reuters.com/sustainability/boards-policy-regulation/south-korean-police-probe-massive-data-leak-coupang-2025-12-01/

• *CISA and Partners Release Advisory Update on Akira Ransomware | CISA*. (2025, November 13). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/alerts/2025/11/13/cisa-and-partners-release-advisory-update-akira-ransomware

• Parikh, H., Nighan, M., Montague, V., Mambwe Mutanuka, & Yang, A. (2025, November 12). *The Change Healthcare cybersecurity breach: Impact on healthcare providers*. Nixon Peabody LLP; Nixon Peabody. https://www.nixonpeabody.com/insights/alerts/2025/11/12/change-healthcare-cybersecurity-breach-impact-on-healthcare-providers

• Vicens, A. J. (2025, December 4). Chinese-linked hackers use back door for potential “sabotage,” US and Canada say. *Reuters*. https://www.reuters.com/world/china/chinese-linked-hackers-use-back-door-potential-sabotage-us-canada-say-2025-12-04/

• CISA. (2023). *Stop Ransomware*. Www.cisa.gov. https://www.cisa.gov/stopransomware

• Sead Fadilpašić. (2025, December). *Millions of footballers see info leaked after French Football Federation suffers data breach*. TechRadar. https://www.techradar.com/pro/security/french-football-federation-suffers-data-breach-that-compromised-club-members-data

• CISA. (n.d.). *Recognize and Report Phishing | CISA*. Www.cisa.gov. https://www.cisa.gov/secure-our-world/recognize-and-report-phishing

• NIST. (2025). *Cybersecurity Framework*. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

• CISA. (n.d.). Turn on Multi-Factor Authentication (MFA). CISA. https://www.cisa.gov/secure-our-world/turn-mfa

• Wickramasinghe, S. (2023, May 18). *SOC Metrics: Security Metrics & KPIs for Measuring SOC Success*. Splunk-Blogs. https://www.splunk.com/en_us/blog/learn/security-operations-metrics.html

• Unit 42. (2025, July 30). *2025 Unit 42 Global Incident Response Report: Social Engineering Edition*. Unit 42. https://unit42.paloaltonetworks.com/2025-unit-42-global-incident-response-report-social-engineering-edition/