“Develop a passion for learning.”

RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

RISK RESPONSE STRATEGIES

This module is an introduction to the standard risk response strategies

- Avoid
- Mitigate
- Transfer
- Accept

TECHNICAL REPORTING

- Operational backbone of IT risk management
    - Aimed at engineers, analysts, architects, and security operators
    - Provides granular, data-rich insight required to understand, mitigate, and prevent risk conditions in complex technology ecosystems
- Executive reporting abstracts risk into strategic language
- Technical reporting focuses on
    - Precision
    - Evidence
    - System-level details
- Enables hands-on experts to take corrective action quickly

PURPOSE OF TECHNICAL REPORTING

- Detect emerging vulnerabilities and operational weaknesses
  - Technical reports document:
    - Zero-day or high-severity vulnerabilities affecting critical systems
    - Weak configuration patterns (e.g., permissive IAM roles, open storage buckets)
    - Drift from security baselines
    - Accumulating technical debt that introduces systemic risk
  - Early detection allows teams to intervene before problems escalate into incidents

PURPOSE OF TECHNICAL REPORTING

- Communicate the status of controls and KPIs/KRIs
  - Provides objective measurements of
    - Preventive controls (patching, access control, network segmentation)
    - Detective controls (logging, monitoring, anomaly detection)
    - Corrective controls (backup recovery, failover readiness)
  - KPIs and KRIs reveal
    - Control degradation
    - Capacity issues
    - Operational health trends
    - The onset of fragility in critical systems
  - For example
    - Rising authentication failures may indicate credential stuffing
    - Increasing backup validation failures may signal latent DR risk

PURPOSE OF TECHNICAL REPORTING

- Support forensic and incident response activities
  - Incident response requires accurate, timestamped, contextualized technical evidence, such as
    - Log sequences
    - Host telemetry
    - IAM events
    - Process execution traces
    - Alert correlation
  - Technical reports consolidate this data into a narrative that helps responders
    - Reconstruct attack paths
    - Validate root causes
    - Understand the blast radius
    - Identify whether threats remain active

PURPOSE OF TECHNICAL REPORTING

- Provide architecture teams with insight into systemic risk patterns
  - Architects need risk data to guide
    - Cloud design
    - Network segmentation strategy
    - Microservice resiliency patterns
    - Identity and access models
    - Data governance structures
  - Technical reporting reveals
    - Repeating incident themes
    - Concentrations of vulnerabilities within an architecture pattern
    - Hotspots where security controls consistently underperform
    - System couplings that amplify risk during failures

PURPOSE OF TECHNICAL REPORTING

- Validate whether technical mitigation plans are effective
  - Mitigation is not “proven” because tasks were performed
  - Mitigation is proven because metrics measure that risk declined
  - Technical reporting validates mitigation effectiveness by measuring
  - Reduction in vulnerability counts
    - Decrease in anomalous activity
    - Improved MTTR/MTTD
    - Strengthened control performance
  - This closes the loop between risk reduction effort and actual reduction in risk exposure

CONTENT – RISK DATA

- Risk IDs
  - Provides traceability and links risk records across systems (risk register, GRC platform)
- Categories
  - Examples
    - Cyber
    - Operational
    - Resilience
    - Third-party
    - Compliance
  - Categorization allows aggregated analysis and governance review
- Severity rankings
  - Derived from
    - Likelihood × Impact scoring
    - Velocity (speed with which risk becomes incident)
    - Control strength
  - Severity informs prioritization and escalation

CONTENT – RISK DATA

- Inherent versus residual risk
  - Shows
    - Inherent risk: What exposure would be with no controls
    - Residual risk: Exposure after controls are applied
  - This gap measures control effectiveness
- Probability, impact and velocity
  - Probability: chance of failure or attack
  - Impact: operational, financial, reputational magnitude
  - Velocity: How fast risk materializes
    - For example: high for cyberattacks, medium for misconfiguration, low for tech debt
- Affected assets with criticality context
  - Example
    - "Affected component: Payment API Gateway (Tier 1 critical business service)"
    - Criticality defines urgency

CONTENT – LOGS AND TELEMETRY

- Telemetry is the ground truth of technical risk reporting
  - It provides objective, time-aligned evidence of abnormal or concerning behavior
- Key telemetry types
  - Authentication logs which reveal
    - Credential abuse
    - Brute-force attempts
    - MFA bypass attempts
    - Suspicious access patterns

CONTENT – LOGS AND TELEMETRY

- Endpoint detection events
  - From EDR platforms (CrowdStrike, SentinelOne)
    - Malware detection
    - Suspicious processes
    - Lateral movement behavior
    - Privilege escalations
- Network anomalies
  - Examples
    - Unusual outbound traffic (potential exfiltration)
    - East-west traffic spikes
    - Unusual ports or protocols
  - These often indicate early-stage compromises

CONTENT – LOGS AND TELEMETRY

- Cloud audit logs
  - CloudTrail, Azure Activity Logs, GCP Audit Logs
    - IAM role changes
    - Policy modifications
    - Permission drift
    - Service account usage patterns
    - Infrastructure-as-Code drift
  - Audit logs are essential for cloud forensics

CONTENT – LOGS AND TELEMETRY

- System performance indicators
  - Operational risk often emerges from
    - CPU/memory saturation
    - Queue depth spikes
    - Latency deviations
    - Storage errors or replication lag
  - Performance telemetry often correlates with resilience risks

CONTENT – THREAT INDICATORS

- Indicators of compromise (IoCs)
  - Examples
    - Malicious IP addresses
    - Hashes of known malware
    - Domains used for command-and-control
    - IoC matches elevate incident severity
- Threat intelligence correlations
  - TI platforms map
    - Vulnerabilities in your environment
    - To active exploitation in the wild
  - If a vulnerability is trending in adversary operations, then risk escalates immediately

CONTENT – THREAT INDICATORS

- Exploit availability
  - CVEs with
    - Public PoC code
    - Active scanning by threat actors
    - Weaponized payloads
  - Represent significantly higher risk
- Malicious domain/IP activity
  - Useful for
    - Detecting beaconing
    - Identifying botnet traffic
    - Detecting phishing and spoofing patterns

CONTENT – THREAT INDICATORS

- Privilege escalation patterns
  - Risk indicator for
    - Insider threat
    - Credential compromise
    - Malware payload execution
  - Threat indicators turn telemetry into interpreted security insights

CONTENT – CONTROL EFFECTIVENESS

- Must measure how well controls are performing, not just list them.
- Patching compliance
  - Broken down by
    - Severity
    - Asset class
    - Exposure level
    - Aging (how long outstanding)
  - A key systemic risk indicator

CONTENT – CONTROL EFFECTIVENESS

- MFA enrollment and enforcement
  - A crucial control for preventing credential compromise
  - Reports must show
    - MFA coverage (%) for privileged vs. non-privileged accounts
    - Exceptions and justifications
- Backup integrity rates
  - Key resilience risk metric
    - Successful restores vs failed
    - Corrupted backups
    - Outdated snapshots

CONTENT – CONTROL EFFECTIVENESS

- Incident response metrics: MTTD/MTTR
    - Reveal
        - Control performance
        - Team readiness
        - Detection quality
- Preventive and detective control test results
    - Includes
        - Vulnerability scans
        - Cloud security posture scans
        - Penetration test results
        - Configuration baseline checks
    - Control effectiveness differentiates controlled risk from uncontrolled risk

REMEDIATION RECOMMENDATIONS

- Once risks and control gaps are identified
  - Technical reporting must guide what to do next
  - Recommendations must be actionable, prioritized, and aligned with business and risk appetite
- Remediation recommendations should offer detailed guidance
- Apply specific patches or configuration changes
  - Examples:
    - Patch for CVE-2024-xxxxx affecting gateway services.
    - Disable legacy SSH ciphers.
    - Remove public ingress from testing VPCs.
  - Recommendations must include
    - Target systems
    - Expected impact
    - Test requirements
    - Roll out constraints or windows

REMEDIATION RECOMMENDATIONS

- Increase logging granularity
    - Often necessary when
        - Current logs are insufficient for forensics
        - Threat behavior requires deeper observability
        - Cloud logs are missing key IAM or network events
    - Examples
        - Enable S3 data event logging
        - Expand Linux auditd scope
        - Increase retention windows

REMEDIATION RECOMMENDATIONS

- Update firewall rules, IAM policies, or network segmentation
  - Examples
    - Restrict service accounts to least privilege
    - Tighten outbound traffic rules
    - Segment workloads into separate subnets or security groups
  - Architectural-level remediation like segmentation significantly reduces blast radius
- Implement new detection logic in SIEM or SOAR
  - Examples
    - Add correlation rules for privilege escalation chaining
    - Tune alert thresholds based on anomaly detection
    - Add automated containment routines (SOAR playbooks)
  - This is how organizations achieve adaptive detection and response

REMEDIATION RECOMMENDATIONS

- Strengthen monitoring thresholds or add KRIs
    - Examples
        - Introduce new KRIs for IAM anomalies
        - Lower latency thresholds for critical services
        - Add capacity saturation KRIs to predict outages
    - Monitoring evolves with threat landscape and architecture maturity

REMEDIATION RECOMMENDATIONS

- Re-architect components to reduce single points of failure
    - Examples
        - Add multi-region replication
        - Replace monolithic services with microservices
        - Introduce circuit breakers, retries, and backpressure mechanisms
        - Move stateful workloads to managed, replicated cloud components
    - Architecture recommendations often require
        - Longer timelines
        - Funding
        - Senior leadership approval
    - But they produce large reductions in systemic operational risk

OPERATIONAL METRICS

- Leading and lagging indicators of team performance, system reliability, and control effectiveness
- Change success rate
  - Low change success rate often correlates with
    - Poor deployment practices
    - Insufficient testing
    - Underlying architectural fragility
  - A high-quality risk report uses change metrics to highlight process risk

OPERATIONAL METRICS

- MTTR / MTTD
  - MTTD (Mean Time to Detect): measures detection quality
  - MTTR (Mean Time to Recover): measures response effectiveness
  - Trends
    - Increasing MTTR indicates resilience degradation
    - Decreasing MTTD indicates improved detection from SIEM/SOAR
- Mean time between incidents (MTBI)
  - Low MTBI indicates
    - Chronic issues
    - Weak controls
    - Architectural inefficiencies
    - Process failures
  - MTBI helps identify fragile systems

OPERATIONAL METRICS

- SLA adherence
  - SLA breaches indicate
    - Operational instability
    - Insufficient capacity
    - Bottlenecks in infrastructure or process
  - SLA metrics are critical for customer-facing services
- Vulnerability remediation time
  - Tracks
    - How fast teams respond to new vulnerabilities
    - Bottlenecks in patching workflow
    - Whether vulnerability backlog is growing
  - High remediation times often indicate:
    - Resource shortages
    - Overly manual processes
    - Competing priorities

OPERATIONAL METRICS

- Capacity headroom metrics
  - Measure how close systems are to performance limits
    - CPU, memory, network saturation
    - Queue depth
    - Storage utilization
    - IOPS capacity
  - Low headroom = high operational risk

OPERATIONAL METRICS

- Drift detection counts (IaC Drift)
  - Infrastructure drift introduces
    - Inconsistency
    - Security exposure
    - Configuration complexity
    - Compliance deviations
  - Frequent drift detection signals a need for
    - Stronger DevOps discipline
    - Better automation
    - Reduced manual intervention

Q&A AND OPEN DISCUSSION