RISK AND RESILIENCE BOOTCAMP

TEKsystems Global Services

WORKFORCE DEVELOPMENT

RISK RESPONSES

This module is an overview on risk responses

RISK RESPONSES

- High-maturity risk programs
  - Operate on the principle that speed and intelligence in decision-making directly influence the severity and spread of incidents
  - In modern distributed architectures risk conditions evolve in minutes, not hours
- Real-time monitoring and rapid escalation
  - Ensure that organizations detect anomalies, evaluate them in context
  - Then mobilize the right resources before risks escalate into operational failures or security breaches

REAL-TIME DECISION DRIVERS

- Real-time decisions are not made ad-hoc
  - They are guided by predefined risk-driven criteria that ensure consistency, compliance, and clear prioritization
- Severity classification (SEV-1 to SEV-4)
  - Organizations classify incidents according to severity levels that determine urgency, staffing, and escalation paths
    - SEV-1: Critical business-impacting outage or security breach. Required 24/7 immediate response
    - SEV-2: Major functional impairment affecting customers or key workflows
    - SEV-3: Limited impact or localized degradation
    - SEV-4: Low priority; informational or minor anomaly
  - Example
    - If authentication API fails → SEV-1 (core service)
    - If internal reporting dashboard slows → SEV-3

REAL-TIME DECISION DRIVERS

- Business impact mapping
  - Driven by RTO, RPO, and criticality ratings from the BIA
  - Systems with tight RTO/RPO require faster alerts and escalations
  - Critical services (payments, trading platforms, identity providers) require immediate action even for small anomalies
  - Non-critical services tolerate slower response
  - Example
    - A 200 ms latency spike in a real-time trading platform may trigger SEV-1
    - A 15-minute delay in a batch report may not

REAL-TIME DECISION DRIVERS

- KRI thresholds (static and dynamic)
  - Real-time KRIs use thresholds configured based on
    - Static values (fixed limits, often regulatory or policy-based)
    - Dynamic models (baselines, ML anomaly detection, z-scores)
  - Examples
    - Static: “Any encryption key reaching expiry within 7 days triggers escalation.”
    - Dynamic: “Alert if login failure rate deviates >3σ from baseline.”

REAL-TIME DECISION DRIVERS

- Policy-defined escalations
- Policies codify
  - Who responds
  - Within what timeframe
  - What mandatory steps are required
  - When escalation to senior leadership is required
  - Which events must be logged for audit purposes
  - Policies ensure decisions remain consistent, defensible, and compliant

REAL-TIME DECISION DRIVERS

- Regulatory reporting triggers
  - Several regulations require near-real-time notification
    - NY DFS Part 500: 72-hour notice for material cybersecurity events
    - GDPR: 72-hour breach reporting
    - PCI DSS: strict timelines for cardholder data incidents
    - FFIEC: Operational resilience guidelines for financial institutions
  - Real-time escalation frameworks must incorporate these deadlines, often requiring automatic flagging when regulatory thresholds are crossed

REAL-TIME TOOLS

- SIEMs
  - SIEM event correlation and detection
  - SIEM = Security Information and Event Management
  - SIEMs aggregate logs and security events
  - Detect threats by correlating multiple signals
  - Identify behavioral anomalies
  - Trigger alerts when risk conditions exceed tolerance
  - Example
    - Combining IAM logs + network patterns can detect detect lateral movement

REAL-TIME TOOLS

- SOAR
  - Security Orchestration, Automation, and Response
  - SOAR platforms automate routine responses
    - Auto-block malicious IPs
    - Quarantine compromised endpoints
    - Trigger MFA challenges
    - Enrich alerts with threat intel
    - Escalate tickets to ServiceNow automatically
  - This dramatically reduces MTTR and human workload

REAL-TIME TOOLS

- Live responder mobilization
  - Used for:
    - Immediate on-call paging
    - Multi-channel alerts (SMS, phone, push)
    - Automated on-call rotations
    - Incident commander activation
  - Critical for SEV-1/SEV-2 incidents

REAL-TIME TOOLS

- Telemetry-driven alerts
  - Sample tools: CloudWatch, Datadog, Prometheus
  - These platforms provide:
    - Real-time metrics (CPU, IOPS, latency)
    - Distributed tracing
    - SLO/SLA monitoring
    - Dynamic alerting based on baselines
  - They detect operational risk events before they propagate

REAL-TIME TOOLS

- Governance-driven escalation
  - ServiceNow / Archer GRC
  - These tools:
    - Create incident or risk records
    - Initiate GRC workflows (Governance, Risk, and Compliance)
    - Manage evidence and documentation
    - Track compliance-related escalations
    - Enforce approvals and accountability
  - They ensure that real-time response is also audit-ready

ESCALATION FRAMEWORK

- A high-maturity organization uses structured, hierarchical escalation to ensure the right people are engaged fast
  - Tier 1: Initial triage
    - Performs basic investigation (check logs, validate alerts)
    - Filters false positives
    - Assigns provisional severity
    - Engages Tier 2 if needed
  - Tier 2 : System/platform SMEs
    - Deep technical analysis (containers, databases, identity, network)
    - Offer architecture-level insights
    - Own resolution of platform-specific issues

ESCALATION FRAMEWORK

- Tier 3: Security analysts / senior engineers
  - Lead investigation into sophisticated threats (malware, lateral movement, data exfiltration)
  - Conduct forensic analysis
  - Coordinate multi-team responses
  - Make containment or shutdown decisions
- Leadership (CIO/CISO)
  - Required for SEV-1 events and regulatory issues
  - Decide on customer notifications, public communication, or legal actions
  - May trigger Business Continuity or Disaster Recovery plans
- Regulators, regulatory notification is often mandatory when in a regulated industry there is
  - Material customer impact
  - Material data exposure
  - Loss of key services
  - Breaches of specific KRIs
  - Security incidents affecting critical infrastructure
  - Escalation to regulators is often time-bound and non-negotiable

REAL-TIME DECISION-MAKING

- Context-aware alerts - asset criticality integration
- Alerts incorporate:
  - Asset importance (tier-1 vs. tier-3 systems)
  - Data sensitivity
  - Business function mapping
  - A CPU spike on a tier-3 staging server ≠ a CPU spike on a core payments service

REAL-TIME DECISION-MAKING

- Dynamic alert suppression (noise reduction)
- High-maturity systems automatically suppress
  - Repeated alerts
  - Low-value anomalies
  - Known benign patterns
  - Flapping metrics
- This reduces “alert fatigue” and allows responders to focus on critical signals

REAL-TIME DECISION-MAKING

- Threat correlation
  - Weak signals may indicate a strong risk event
- Multiple low-severity anomalies might indicate
  - Coordinated attack
  - Insider threat behavior
  - Critical system degradation
  - Misconfigured infrastructure
- Examples
  - Failed logins + unusual IP + privilege escalation attempt might indicate possible credential compromise
  - Memory pressure + network latency + container restarts might indicate impending service outage

REAL-TIME DECISION-MAKING

- AI-Assisted Decision Support
- Advanced platforms apply ML models to
  - Predict severity based on historical patterns
  - Suggest probable root causes
  - Recommend containment actions
  - Score risk levels in real time
  - Identify correlated alerts across services
- This augments human expertise with intelligent prioritization

Q&A AND OPEN DISCUSSION