==========

TENABLE + SERVICENOW HYBRID VULNERABILITY MANAGEMENT

Implementation Guide & Business Case

==========

EXECUTIVE SUMMARY

This document outlines a high-margin consulting opportunity combining commercial off-the-shelf (COTS) platforms with custom integration services. By reselling Tenable and ServiceNow licenses at markup and building custom integrations, consulting firms can achieve 55-65% gross margins while delivering enterprise-grade vulnerability management solutions.

THE OPPORTUNITY AT A GLANCE:

- COTS Revenue: Resell Tenable + ServiceNow at 25-40% markup
- Custom Integration: $40K-80K per implementation (3-6 weeks effort)
- Recurring Services: $5K-15K/month for ongoing support
- Total Year 1 Revenue: $250K-450K per mid-market client
- Gross Margin: 55-65%

THE MARKET CONTEXT:

ServiceNow developer demand is exploding, with projections showing demand will exceed supply by 2025. There are currently thousands of ServiceNow engineer positions open globally, with consulting rates ranging from $150-300/hour. The ServiceNow Vulnerability Response module specifically is identified as a high-demand specialization, with SecOps professionals commanding premium rates.

==========

SECTION 1: THE TECHNICAL SOLUTION

==========

ARCHITECTURE OVERVIEW

The solution combines three components:

1. TENABLE (Vulnerability Scanning Platform)
   - Tenable.io for cloud/SaaS scanning
   - Tenable.sc (Security Center) for on-premise scanning
   - Tenable.cs for container/cloud-native scanning

2. SERVICENOW (CMDB + Workflow Automation)
   - ServiceNow CMDB for asset inventory

• ServiceNow Vulnerability Response module
• ServiceNow ITSM for ticketing and workflow

3. CUSTOM INTEGRATION LAYER (Our Value-Add)
• Automated vulnerability-to-asset mapping
• Custom ownership resolution logic
• Intelligent ticket routing and creation
• SLA enforcement and escalation workflows
• Executive dashboards and reporting

HOW IT WORKS: END-TO-END FLOW

STEP 1: Scanning & Discovery
• Tenable scans infrastructure (on-prem, cloud, containers)
• Discovers vulnerabilities with CVE details, CVSS scores, affected hosts
• Exports findings via API

STEP 2: Integration & Enrichment (OUR CUSTOM LAYER)
• ServiceNow base integration imports Tenable findings
• OUR custom integration:
  - Matches Tenable assets to ServiceNow CMDB Configuration Items (CIs)
  - Enriches vulnerabilities with business context (criticality, owner, env)
  - Deduplicates findings across multiple Tenable instances
  - Applies custom risk scoring based on client-specific factors
  - Filters out accepted risks and false positives

STEP 3: Vulnerable Item Creation
• System creates Vulnerable Items (VIs) in ServiceNow
• VIs linked to specific Configuration Items in CMDB
• VIs inherit ownership and business context from CIs

STEP 4: Automated Ticket Creation & Routing (OUR CUSTOM WORKFLOW)
• Custom business rules trigger ticket creation based on severity + context
• Tickets automatically assigned to correct service owners from CMDB
• Assignment groups determined by:
  - CI ownership (from CMDB)
  - Service mapping (business service → IT service → CI)
  - Custom routing rules (client-specific)

STEP 5: Workflow Automation
• SLA clock starts automatically
• Escalation notifications triggered at defined thresholds
• Remediation tasks created with fix guidance
• Progress tracked in ServiceNow dashboards

STEP 6: Validation & Closure
• Once remediated, validation workflow triggers
• Options for validation:
  - Automatic re-scan in Tenable
  - Manual evidence submission
  - Approval workflow for risk acceptances
• Ticket automatically closed only after validation

OUT-OF-BOX VS. CUSTOM INTEGRATION

SERVICENOW BASE INTEGRATION (Available on ServiceNow Store):
✓ Imports Tenable vulnerability data
✓ Creates Third-Party Vulnerabilities and Vulnerable Items
✓ Basic field mapping (CVE, CVSS, host info)
✓ Scheduled import jobs
✓ Manual asset matching

GAPS IN BASE INTEGRATION:
✗ No automatic ownership resolution
✗ No business context enrichment
✗ Generic ticket creation (all goes to one queue)
✗ No custom prioritization logic
✗ No validation workflows
✗ Limited deduplication
✗ Basic reporting only

OUR CUSTOM INTEGRATION LAYER ADDS:

1. INTELLIGENT OWNERSHIP MAPPING
• Automatic match: Tenable host → ServiceNow CI → Service Owner
• Uses multiple data sources:
  - CMDB relationships
  - Business Service maps
  - Cloud resource tags (AWS/Azure)
  - Active Directory groups
  - Custom ownership tables
• Confidence scoring when matches are ambiguous
• Escalation to security team for unmatched assets

2. CONTEXT-AWARE PRIORITIZATION
• Beyond CVSS scoring, incorporates:
  - Internet exposure (public vs. internal)
  - Data classification (PII, PCI, PHI)

- Business criticality (from CMDB)
- Exploit availability (from threat intel)
- Regulatory requirements
- Environment type (prod vs. dev)

• Outputs custom risk score: 1-100

3. INTELLIGENT TICKET ROUTING

• Creates tickets in appropriate teams' queues
• Includes all necessary context:
- Business impact explanation
- Fix guidance and resources
- SLA deadline and justification
- Links to CI, VI, and CVE details
• Avoids ticket overload:
- Groups related vulnerabilities
- Creates single ticket for multiple instances of same vuln
- Suppresses findings per policy (e.g., dev environments)

4. SLA ENFORCEMENT ENGINE

• Custom SLA policies by severity + asset type:
- Critical + Production: 7 days
- High + Production: 30 days
- Critical + Dev: 30 days
- etc.
• Automated escalation chains:
- Day 3: Reminder to assignee
- Day 5: Escalate to team lead
- Day 7: Escalate to director
- SLA breach: Executive notification
• Prevents SLA gaming with validation requirements

5. VALIDATION WORKFLOWS

• Multi-option validation:
- Auto-trigger Tenable re-scan on closure
- Require evidence upload
- Manual security team approval
• Prevents premature closure
• Tracks false closures and reopens tickets
• Historical tracking of recurring vulnerabilities

6. EXECUTIVE DASHBOARDS

• Real-time visibility into:
- Open critical vulnerabilities by business unit
- MTTR trending
- SLA compliance %

  - Risk score by service
  - Team performance metrics
• Drill-down capability from summary to individual VIs
• Automated weekly/monthly reports
• Mobile-accessible

REAL-WORLD IMPLEMENTATION EXAMPLE

Healthcare Company (800 employees, HIPAA-regulated):

ENVIRONMENT:
• 500 servers (mix of on-prem and AWS)
• 200 applications
• Tenable.sc for on-prem, Tenable.io for cloud
• ServiceNow already in use for ITSM
• CMDB partially populated

CHALLENGES:
• 800+ vulnerabilities discovered weekly
• No clear ownership for 60% of assets
• Security team manually creating tickets
• Engineering teams ignoring generic security tickets
• Auditors requiring evidence of remediation within SLA

OUR IMPLEMENTATION:

Phase 1 (Week 1-2): Discovery & Design
• Interviewed 15 stakeholders
• Mapped CMDB coverage and gaps
• Documented approval workflows
• Designed ownership mapping logic
• Created custom SLA matrix

Phase 2 (Week 3-4): ServiceNow Configuration
• Installed Vulnerability Response module ($40K/year)
• Configured base Tenable integration
• Set up CMDB CI classes and relationships
• Created custom tables for ownership mapping
• Built assignment group structure

Phase 3 (Week 5-8): Custom Integration Development
• Built ownership resolution engine:
  - Tenable asset → ServiceNow CI matching (90% auto-match)
  - Cloud tag → CMDB enrichment

- Manual override UI for exceptions

• Developed custom risk scoring:
- HIPAA-regulated systems: 2x multiplier
- Public-facing services: 1.5x multiplier
- Dev/test environments: 0.5x multiplier

• Created intelligent routing:
- Infrastructure vulns ⟹ System Admin team
- Application vulns ⟹ Dev team by app
- Database vulns ⟶ DBA team
- Cloud vulns ⟶ Cloud Engineering team

• Built SLA enforcement:
- Critical/HIPAA: 14 days
- High/HIPAA: 30 days
- Automated escalations with custom email templates

• Implemented validation workflow:
- Auto-rescan on closure
- Security team approval for risk acceptances
- Evidence requirement for manual fixes

Phase 4 (Week 9-10): Testing & Training
• UAT with 10 users across teams
• Training for security team (4 hours)
• Training for IT teams (2 hours)
• Documentation and runbooks

Phase 5 (Week 11-12): Go-Live & Optimization
• Cutover from manual process
• Monitor first 100 vulnerabilities
• Tune scoring and routing rules
• Address edge cases

RESULTS AFTER 6 MONTHS:
• Time to identify owner: 4 hours ⟶ 2 minutes (99% reduction)
• Tickets created: 800/week ⟶ 150/week (proper grouping)
• Ticket response rate: 40% ⟹ 85%
• MTTR for critical: 45 days ⟹ 12 days (73% reduction)
• SLA compliance: 35% ⟶ 88%
• Audit prep time: 40 hours ⟶ 3 hours per cycle

CLIENT TESTIMONIAL:
"Before, we were drowning in vulnerabilities with no clear way to track who was

responsible. Now, the system automatically knows who owns what and creates tickets for the right teams. Our audit last month was the smoothest we've ever had - we pulled reports in minutes that used to take days to compile."
- CISO, Mid-market Healthcare Company

==========

SECTION 2: BUSINESS MODEL & PRICING

==========

REVENUE COMPONENTS

Our revenue comes from three sources:

1. PLATFORM LICENSING (Resale with Markup)
2. CUSTOM INTEGRATION (One-time Implementation Services)
3. MANAGED SERVICES (Recurring Monthly Revenue)

DETAILED PRICING BREAKDOWN

1. PLATFORM LICENSING (Annual, with 30% markup)

TENABLE LICENSING:
• Wholesale cost (estimated):
  - Tenable.io: ~$2,500 per year per scanner
  - Tenable.sc: ~$15,000-50,000 per year (based on IP count)
  - Average mid-market: ~$35,000/year wholesale

• Our resale price: $45,500/year
• Our margin: $10,500/year (30%)

SERVICENOW LICENSING:
• ServiceNow Vulnerability Response module: ~$40,000/year wholesale
• Our resale price: $52,000/year
• Our margin: $12,000/year (30%)

If client already has ServiceNow ITSM:
• Just add Vulnerability Response: $40K wholesale → $52K our price
• Margin: $12K/year

If client needs full ServiceNow:
• ITSM base + Vulnerability Response: ~$80K/year wholesale
• Our resale: $104K/year
• Our margin: $24K/year

TOTAL PLATFORM REVENUE (Year 1):
• Scenario A (Client has ServiceNow): $97,500
• Scenario B (New ServiceNow): $149,500
• Our margin: $22,500-34,000

2. CUSTOM INTEGRATION SERVICES (One-time)

Our billable implementation hours at $200/hour blended rate:

DISCOVERY & DESIGN (80-120 hours):
• Stakeholder interviews: 20 hours
• CMDB assessment: 16 hours
• Workflow documentation: 24 hours
• Architecture design: 20 hours
• SLA policy definition: 10 hours
• Project planning: 10 hours
Total: 100 hours × $200 = $20,000

CONFIGURATION & DEVELOPMENT (200-300 hours):
• ServiceNow module setup: 40 hours
• Base Tenable integration: 20 hours
• CMDB enhancement: 30 hours
• Ownership mapping logic: 60 hours
• Custom risk scoring: 40 hours
• Ticket routing rules: 30 hours
• SLA enforcement: 30 hours
• Validation workflows: 30 hours
• Dashboard development: 20 hours
Total: 300 hours × $200 = $60,000

TESTING & TRAINING (60-80 hours):
• UAT coordination: 20 hours
• Bug fixes and tuning: 20 hours
• Training development: 10 hours
• Training delivery: 10 hours
• Documentation: 10 hours
Total: 70 hours × $200 ≡ $14,000

GO-LIVE & OPTIMIZATION (40-60 hours):
• Cutover support: 20 hours
• Initial monitoring: 20 hours
• Rule tuning: 10 hours
Total: 50 hours × $200 = $10,000

TOTAL IMPLEMENTATION SERVICES: $104,000

Typical range for mid-market: $80K-130K
Enterprise (more complexity): $150K-250K

COST STRUCTURE:

Labor costs (our actual cost):
• Senior consultant: $120/hour × 120 hours = $14,400
• Integration developer: $90/hour × 280 hours = $25,200
• Junior consultant: $60/hour × 120 hours = $7,200
Total labor cost: $46,800

Project overhead (15%): $7,020
Total cost: $53,820

MARGIN ON SERVICES: $104,000 - $53,820 = $50,180 (48% margin)

3. MANAGED SERVICES (Recurring Monthly)

TIER 1: PLATFORM MANAGEMENT ($7,500/month ≡ $90K/year)
• ServiceNow admin support (20 hours/month)
• Tenable scanner maintenance
• Integration health monitoring
• User provisioning
• Monthly status reports
• Emergency support (4-hour SLA)

TIER 2: ACTIVE MANAGEMENT ($12,500/month = $150K/year)
• Everything in Tier 1
• Quarterly optimization reviews
• New scanner integrations
• Workflow enhancements
• Policy updates
• Integration of new assets
• 40 hours/month support

TIER 3: STRATEGIC PARTNERSHIP ($20,000/month = $240K/year)
• Everything in Tier 2
• Dedicated consultant (0.5 FTE)
• Continuous improvement roadmap
• Advanced analytics

• Executive business reviews
• Unlimited support

COST STRUCTURE (Tier 2 example):
• Labor: $90/hour × 50 hours/month = $4,500/month
• Platform monitoring tools: $500/month
• Total cost: $5,000/month

MARGIN: $12,500 - $5,000 ≡ $7,500/month (60% margin)

COMPLETE CLIENT ECONOMICS

MID-MARKET CLIENT (800 employees, already has ServiceNow):

YEAR 1:
Revenue:
• Platform licenses: $97,500
• Implementation: $104,000
• Managed services (Tier 2): $150,000 (starting month 4)
• Total Year 1 revenue: $351,500

Costs:
• Platform wholesale: $75,000
• Implementation labor: $53,820
• Managed services: $45,000 (9 months)
• Total Year 1 costs: $173,820

YEAR 1 PROFIT: $177,680 (51% margin)

YEAR 2+:
Revenue:
• Platform licenses: $97,500
• Managed services: $150,000
• Total Year 2+ revenue: $247,500

Costs:
• Platform wholesale: $75,000
• Managed services: $60,000
• Total Year 2+ costs: $135,000

YEAR 2+ PROFIT: $112,500 (45% margin)

3-YEAR TOTAL:
• Revenue: $846,500

• Costs: $443,820
• Profit: $402,680 (48% average margin)

==========

SECTION 3: THE SERVICENOW DEVELOPER MARKET

==========

MASSIVE MARKET DEMAND

The ServiceNow ecosystem is experiencing explosive growth:

MARKET SIZE:
• ServiceNow revenue projected: $15B+ by 2025
• Market growth rate: 22% CAGR through 2028
• Demand for professionals will EXCEED supply by 2025

JOB MARKET DATA:
• Thousands of ServiceNow engineer positions open globally
• Indeed shows 8,000+ ServiceNow developer jobs in US alone
• LinkedIn shows 15,000+ ServiceNow positions worldwide

SALARY RANGES (US Market):
• Entry-level Admin: $75K-90K
• Mid-level Developer: $100K-140K
• Senior Developer/Consultant: $140K-200K
• Architect: $180K-280K

CONSULTING RATES:
• Junior consultant: $80-120/hour
• Mid-level consultant: $150-200/hour
• Senior consultant/architect: $225-300/hour
• Blended team rate: $150-250/hour

WHY SERVICENOW SKILLS ARE VALUABLE

1. PLATFORM COMPLEXITY
   • Requires JavaScript, REST APIs, relational databases
   • Integration patterns with enterprise systems
   • Security and compliance expertise

2. DOMAIN EXPERTISE
   • ITSM processes (ITIL framework)
   • Security operations workflows

- HR service delivery
- GRC and compliance

3. MODULE SPECIALIZATION
- High-demand modules: SecOps, ITOM, HRSD, GRC
- Vulnerability Response specifically in-demand
- Integration Hub expertise

4. CERTIFICATION VALUE
- CSA (Certified System Administrator): Entry requirement
- CAD (Certified Application Developer): Core for developers
- CIS (Certified Implementation Specialist): Premium rates

5. LOW-CODE OPPORTUNITY
- ServiceNow embracing low-code/no-code
- Faster development, more accessible
- Business + technical skills combination valuable

SERVICENOW SECOPS/VULNERABILITY RESPONSE SPECIALIZATION

The Vulnerability Response module is specifically mentioned as HIGH-DEMAND:

MARKET DRIVERS:
- Regulatory compliance requirements increasing
- Cyber insurance requiring vulnerability programs
- Board-level attention to cyber risk
- Breach costs driving investment

SKILLS IN DEMAND:
- Vulnerability management domain expertise
- Integration with scanning tools (Tenable, Qualys, Rapid7)
- Threat intelligence integration
- Automation and orchestration
- Compliance reporting

TYPICAL PROJECT TYPES:
- Initial VR module implementation: $50K-150K
- Scanner integrations: $30K-80K each
- Custom workflow development: $40K-100K
- Remediation orchestration: $60K-120K
- Compliance automation: $50K-100K

CLIENT TYPES:
- Healthcare (HIPAA compliance)

• Financial services (PCI-DSS, SOC 2)
• Government contractors (NIST 800-53)
• Any regulated industry

WHY THE TENABLE + SERVICENOW COMBO IS LUCRATIVE

1. BOTH ARE MARKET LEADERS
- Tenable: #1 vulnerability management platform
- ServiceNow: #1 ITSM/workflow platform
- Both have large installed bases

2. PRE-EXISTING CUSTOMERS
- Many enterprises already have one or both
- Easier to upsell integration than new platforms
- Familiar with vendors

3. KNOWN INTEGRATION PATTERN
- ServiceNow Store has base integration
- Proof of concept readily available
- Reduces perceived risk

4. CLEAR VALUE PROPOSITION
- Automated workflow ≡ measurable time savings
- Improved SLA compliance ≡ audit success
- Better visibility = executive buy-in

5. RECURRING REVENUE
- Both are subscription platforms
- Annual renewals mean ongoing relationship
- Opportunity for continuous optimization

REAL-WORLD RATE EXAMPLE

A consultant we know charged $60K for a Tenable-ServiceNow integration:

PROJECT SCOPE:
• Client already had both Tenable and ServiceNow
• Needed automated ticket creation
• Simple ownership mapping using CMDB
• Basic SLA tracking

TIME SPENT:
• Discovery: 1 week

• Development: 3 weeks
• Testing/training: 1 week
• Total: ~200 hours actual work

EFFECTIVE RATE: $60,000 / 200 hours = $300/hour

CONSULTANT'S COST:
• Solo consultant, no overhead
• Approximate cost: $30-40/hour (opportunity cost)
• Profit: $52,000-56,000 (87-93% margin)

This demonstrates the profitability of these integrations, especially for experienced consultants who can work efficiently.

==========

SECTION 4: BUILDING YOUR SOFTWARE PORTFOLIO

==========

THE STRATEGIC VALUE OF REUSABLE COMPONENTS

Every custom integration we build becomes a reusable asset:

FIRST CLIENT: Healthcare Company
• Build ownership mapping engine: $60K (300 hours)
• Build risk scoring framework: $40K (200 hours)
• Build validation workflows: $30K (150 hours)
• Total custom development: $130K
• Client pays full cost
• We own the IP

SECOND CLIENT: Financial Services Company
• Ownership mapping: Configure for their env (80 hours) = $16K
• Risk scoring: Adjust for PCI requirements (60 hours) = $12K
• Validation: Minor tweaks (30 hours) = $6K
• Total: $34K (70% code reuse)
• Margin improves: 48% → 65%

THIRD CLIENT: Technology Company
• Ownership mapping: Quick config (40 hours) = $8K
• Risk scoring: Use existing, tune (30 hours) = $6K
• Validation: Minimal changes (15 hours) = $3K
• Total: $17K (85% code reuse)
• Margin improves: 65% → 75%

FOURTH+ CLIENTS:

- Largely configuration vs. development
- 90%+ code reuse
- Margins approach 80%

COMPONENTIZED ARCHITECTURE

We build modular, reusable components:

1. OWNERSHIP RESOLUTION ENGINE

- Input: Tenable asset data (hostname, IP, cloud tags)
- Processing: Match against CMDB CIs using multiple algorithms
- Output: CI sys_id + owner + confidence score
- Reusable across all clients
- Configuration: Client-specific matching rules

2. RISK SCORING FRAMEWORK

- Input: Vulnerability data + asset context
- Processing: Weighted scoring model
- Output: Custom risk score (1-100)
- Reusable calculation engine
- Configuration: Client-specific weights and multipliers

3. TICKET ROUTING ENGINE

- Input: Vulnerable Item + risk score
- Processing: Business rules for assignment
- Output: Assignment group + priority
- Reusable rules engine
- Configuration: Client-specific routing table

4. SLA ENFORCEMENT ENGINE

- Input: Ticket creation + severity + asset type
- Processing: SLA calculation and escalation logic
- Output: Due dates + escalation schedule
- Reusable policy engine
- Configuration: Client-specific SLA matrix

5. VALIDATION WORKFLOW FRAMEWORK

- Input: Ticket closure attempt
- Processing: Validation requirements check
- Output: Approval/rejection + actions
- Reusable workflow templates
- Configuration: Client-specific validation rules

6. DASHBOARD FRAMEWORK
- Input: VI and ticket data
- Processing: Aggregations and calculations
- Output: Executive dashboards
- Reusable visualization templates
- Configuration: Client-specific KPIs

TECHNICAL APPROACH FOR REUSABILITY

ServiceNow provides excellent platforms for reusable code:

UPDATE SETS:
- Package entire configurations
- Export/import across instances
- Version control
- Easy deployment

SCOPED APPLICATIONS:
- Isolated namespace
- Can be installed in any instance
- Marketplace distribution potential
- Licensing opportunities

INTEGRATION HUB SPOKES:
- Reusable integration components
- Flow Designer compatible
- Can be shared across clients

BEST PRACTICES:
- Configuration over customization
- Property-driven behavior
- Client-specific data in tables, not code
- Comprehensive documentation
- Automated testing

PATH TO PRODUCTIZATION

PHASE 1: Service (Years 1-2)
- 5-10 custom implementations
- Build core component library
- Document patterns and anti-patterns
- Revenue: $500K-2M

PHASE 2: Accelerators (Years 2-3)
• Package components as "accelerators"
• Offer fixed-price implementations
• 80% pre-built, 20% custom
• Revenue: $2M-5M

PHASE 3: Product (Years 4-5)
• Launch as ServiceNow Store app
• Subscription + implementation services
• Partner program for other consultants
• Revenue: $5M-15M

EXIT OPTIONS:
• Continue as services business (good lifestyle)
• Pivot to product company (scale opportunity)
• Acquire complementary capabilities
• Sell to larger consulting firm or PE (3-5x revenue)
• Sell to ServiceNow or Tenable (strategic acquisition)

IP PORTFOLIO VALUATION

After 10 implementations, we have:
• Battle-tested components (500+ hours development)
• Proven ROI case studies
• Reference customers
• Recurring revenue base

VALUATION METHODS:

1. Cost Replacement Value
   • 500 hours × $200/hour = $100K development cost
   • Represents minimum value

2. Revenue Multiple
   • $2M annual revenue from implementations
   • SaaS companies: 5-10x revenue
   • Services companies: 0.5-2x revenue
   • Hybrid: 2-4x revenue = $4M-8M

3. Profit Multiple
   • $1M annual profit
   • EBITDA multiple: 3-6x
   • Valuation: $3M-6M

4. Strategic Value
   • ServiceNow partner ecosystem valuable
   • Tenable partnership valuable
   • Customer relationships valuable
   • Premium could be 20-50% above financial metrics

==

SECTION 5: GO-TO-MARKET STRATEGY

==

TARGET CUSTOMER PROFILE

IDEAL CUSTOMERS:
• 500-5,000 employees
• Already using Tenable OR ServiceNow (easier sell)
• Regulated industry (healthcare, financial, government)
• Active vulnerability management program
• Pain points we solve:
  - Manual ticket creation
  - Unclear ownership
  - Poor SLA compliance
  - Audit challenges

BUYER PERSONAS:

1. CISO / VP Security (Economic Buyer)
   • Wants: Improved MTTR, audit success, board reporting
   • Pain: Can't demonstrate security posture
   • Message: "Automated vulnerability-to-remediation workflow"

2. Vulnerability Manager (Primary User)
   • Wants: Less manual work, better tracking
   • Pain: Spending 20+ hours/week on manual coordination
   • Message: "Eliminate manual ticket creation and follow-up"

3. IT Director (Influencer/User)
   • Wants: Clear priorities, less noise
   • Pain: Security sends generic tickets that get ignored
   • Message: "Your teams only see relevant, contextualized tickets"

4. Compliance Manager (Influencer)
   • Wants: Audit evidence, policy enforcement
   • Pain: Manual evidence collection takes 40+ hours
   • Message: "One-click audit reports with full evidence trail"

LEAD GENERATION STRATEGIES

1. SERVICENOW ECOSYSTEM
- List on ServiceNow Store (as partner)
- ServiceNow partner program
- ServiceNow user groups and events
- ServiceNow Knowledge conference

2. TENABLE ECOSYSTEM
- Tenable partner program
- Joint webinars with Tenable
- Tenable user community

3. DIRECT OUTREACH
- LinkedIn targeting ServiceNow admins
- LinkedIn targeting vulnerability managers
- Cold email to CISOs in target industries

4. CONTENT MARKETING
- Blog: "How to Automate Vulnerability Remediation"
- White paper: "Tenable + ServiceNow Integration Guide"
- Case studies with ROI metrics
- YouTube: Tutorial videos

5. SPEAKING ENGAGEMENTS
- ServiceNow Knowledge conference
- Security conferences (RSA, Black Hat)
- Industry events (Healthcare IT, FS-ISAC)
- Local ISSA/ISC2 chapters

6. PARTNERSHIPS
- ServiceNow consulting partners
- Tenable resellers
- MSPs and MSSPs
- GRC consultancies

SALES PROCESS

STAGE 1: Initial Contact
- Pain point discovery call (30 min)
- Qualify: Budget, Authority, Need, Timeline
- If qualified → Schedule technical deep-dive

STAGE 2: Technical Discovery (2-3 hours)
• Demo our integration
• Document their environment
• Map their workflows
• Identify pain points
• Build ROI model
• Deliverable: Assessment summary (15 pages)

STAGE 3: Proposal (1 week)
• Detailed architecture diagram
• Implementation plan with timeline
• Pricing broken down by component
• ROI calculation
• References and case studies
• Deliverable: Formal proposal (30 pages)

STAGE 4: Contracting (2-4 weeks)
• Negotiate terms
• SOW finalization
• Purchase orders
• Kickoff scheduled

TYPICAL SALES CYCLE:
• Small/Mid-market: 4-8 weeks
• Enterprise: 3-6 months

PRICING & PACKAGING

PACKAGE 1: "Quick Start" ($120K)
• For: Companies with both platforms already
• Includes:
  - Basic ownership mapping
  - Automated ticket creation
  - Simple SLA tracking
  - 30 days implementation
  - 3 months support
• Best for: Smaller teams, simple environments

PACKAGE 2: "Enterprise" ($220K)
• For: Companies needing comprehensive solution
• Includes:
  - Advanced ownership mapping
  - Custom risk scoring

- Validation workflows
- Executive dashboards
- 12 weeks implementation
- 6 months support

• Best for: Mid-market, regulated industries

PACKAGE 3: "Platinum" ($350K+)

• For: Large enterprises, complex environments
• Includes:
- Everything in Enterprise
- Multiple scanner integrations
- Multi-tenant configuration
- Advanced compliance reporting
- 16+ weeks implementation
- 12 months support
- Quarterly optimization reviews

• Best for: Fortune 1000, highly regulated

ADD-ONS:

• Additional scanner integration: $30K
• Custom reporting module: $20K
• Training (per day): $3K
• Extended support: $10K-20K/month

COMPETITIVE POSITIONING

VS. DIY (Client builds themselves):

• Our advantage: Pre-built components, proven patterns
• Time to value: 3 months vs. 12+ months
• Risk: Low (references) vs. High (unknown unknowns)
• Cost: Lower (reusable code) vs. Higher (from scratch)

VS. GENERAL SERVICENOW CONSULTANTS:

• Our advantage: Vulnerability management domain expertise
• Components: Pre-built vs. Build from scratch
• Risk scoring: Proven algorithms vs. Generic CVSS
• References: Specific use case vs. Generic ITSM

VS. SECURITY CONSULTANCIES:

• Our advantage: ServiceNow development expertise
• Speed: Fast (know the platform) vs. Learning curve
• Quality: Production-grade code vs. POC-quality
• Support: Ongoing platform expertise vs. Hand-off

VS. PLATFORM VENDORS (ServiceNow/Tenable):
• Our advantage: Independence and customization
• Customization: Deep and flexible vs. Limited
• Cost: Competitive rates vs. Premium pricing
• Support: Dedicated consultant vs. Shared resources

==========

SECTION 6: IMPLEMENTATION METHODOLOGY

==========

STANDARD IMPLEMENTATION TIMELINE (12 weeks)

WEEK 1-2: DISCOVERY & DESIGN
Activities:
• Kickoff meeting with stakeholders
• Environment assessment (Tenable, ServiceNow, CMDB)
• Workflow documentation (current state)
• Pain point deep-dive interviews
• Data quality assessment
• SLA policy workshop
• Ownership mapping strategy
• Architecture design

Deliverables:
• Current state documentation
• Requirements document
• Architecture diagram
• Implementation plan
• Risk register

WEEK 3-4: FOUNDATION BUILD
Activities:
• ServiceNow module installation/configuration
• CMDB enhancement and cleanup
• User/group structure setup
• Base Tenable integration config
• Test data import
• Development environment setup

Deliverables:
• Configured ServiceNow instance (dev)
• CMDB baseline
• Integration credentials validated
• Test import successful

WEEK 5-6: CUSTOM DEVELOPMENT (Ownership & Scoring)

Activities:

- Ownership mapping logic development
- Asset matching algorithms
- Confidence scoring implementation
- Risk scoring framework
- Custom field additions
- Business rules development

Deliverables:

- Ownership resolution engine (v1)
- Risk scoring calculator
- Test results showing 80%+ accuracy

WEEK 7-8: WORKFLOW AUTOMATION

Activities:

- Ticket creation rules
- Assignment logic
- SLA enforcement workflows
- Escalation notifications
- Email templates
- Validation workflow

Deliverables:

- Automated ticket creation working
- SLA tracking operational
- Escalations configured
- Test scenarios passed

WEEK 9-10: REPORTING & TUNING

Activities:

- Dashboard development
- Report creation
- Rule tuning based on test data
- Performance optimization
- Documentation

Deliverables:

- Executive dashboards
- Operational reports
- Tuned rules achieving 90%+ accuracy
- Administrator guide
- User guide

WEEK 11: TRAINING & UAT

Activities:

- Administrator training (4 hours)
- Security team training (2 hours)
- IT team training (2 hours)
- UAT with real users
- Bug fixes
- Final tuning

Deliverables:

- Trained users
- UAT signoff
- Final bug fixes complete

WEEK 12: GO-LIVE & HANDOFF

Activities:

- Production deployment
- Cutover from manual process
- Go-live monitoring
- Issue resolution
- Handoff to support team

Deliverables:

- Production system live
- Support handoff complete
- Project closure

RISK MANAGEMENT

TOP IMPLEMENTATION RISKS & MITIGATIONS:

RISK 1: Poor CMDB data quality

- Impact: Ownership mapping fails
- Probability: High (common issue)
- Mitigation:
  - CMDB assessment in discovery
  - Data cleanup in scope
  - Manual override workflow
  - Phased rollout to test
- Budget: Add 20% contingency for cleanup

RISK 2: Complex organizational structure

- Impact: Routing rules become complicated
- Probability: Medium

• Mitigation:
  - Detailed org chart review
  - Flexible routing table design
  - Default assignment group
  - Escalation to security team
• Budget: Add 40 hours for complex orgs

RISK 3: Integration performance issues
• Impact: Slow imports, system lag
• Probability: Low with proper design
• Mitigation:
  - Performance testing in UAT
  - Batch processing design
  - Off-hours scheduling
  - ServiceNow performance tuning
• Budget: Include in base scope

RISK 4: User adoption challenges
• Impact: Teams ignore tickets
• Probability: Medium
• Mitigation:
  - Executive sponsorship
  - Communication plan
  - Training emphasis
  - Quick wins first
  - Pilot with friendly team
• Budget: Include change management

RISK 5: Scope creep
• Impact: Timeline and budget overruns
• Probability: High (always a risk)
• Mitigation:
  - Clear SOW
  - Change control process
  - Phase 2 parking lot
  - Regular status updates
• Budget: 10% contingency

SUCCESS METRICS

Define success criteria upfront:

OPERATIONAL METRICS:
• Ownership identification time: Target <5 minutes (from hours)

• Ticket volume: Reduce by 60% (through proper grouping)
• Ticket response rate: >80% (from <50%)
• MTTR for critical: <14 days (from 45+ days)
• SLA compliance: >85% (from <50%)

BUSINESS METRICS:
• Audit prep time: Reduce by 80% (40 hours → 8 hours)
• Security team time savings: 15+ hours/week
• IT team satisfaction: Survey score ≥4/5
• Executive visibility: Dashboard usage ≥2x/week

TECHNICAL METRICS:
• Auto-ownership match rate: >85%
• Integration uptime: >99.5%
• Report generation time: <5 seconds
• System performance: No user complaints

==========

SECTION 7: CASE STUDIES & ROI

==========

CASE STUDY 1: HEALTHCARE (800 employees)

CLIENT PROFILE:
• Regional hospital system
• 500 servers, 200 applications
• HIPAA compliance required
• Had: Tenable.sc, ServiceNow ITSM
• Pain: Manual processes, poor audit results

IMPLEMENTATION:
• Duration: 10 weeks
• Cost: $185K (implementation + first year support)
• Team: 2 consultants, part-time

RESULTS AFTER 6 MONTHS:
Operational:
• Ownership ID time: 4 hours → 2 minutes
• Weekly tickets: 800 → 180 (proper grouping)
• Ticket response rate: 40% → 85%
• Critical MTTR: 45 days → 12 days
• SLA compliance: 35% → 88%

Business:

• Audit prep: 40 hours → 3 hours
• Security team time saved: 18 hours/week
• IT satisfaction: 3.2/5 → 4.5/5
• Failed audit findings: 8 → 0

ROI CALCULATION:
Cost:
• Implementation: $135K
• Year 1 support: $50K
• Total: $185K

Savings:
• Security team time: 18 hrs/wk × $75/hr × 52 wks = $70,200
• Audit prep: 37 hrs × 4 audits × $100/hr = $14,800
• Faster remediation (breach prevention): Priceless
• TOTAL QUANTIFIED SAVINGS: $85,000/year

Payback period: 2.2 years
3-year ROI: 37% ($255K savings / $185K investment)

INTANGIBLES:
• Improved security posture
• Better cross-team collaboration
• Executive confidence
• Reduced compliance risk

CASE STUDY 2: FINANCIAL SERVICES (2,000 employees)

CLIENT PROFILE:
• Regional bank
• 1,200 servers, 400 applications
• SOC 2 Type II, PCI-DSS compliance
• Had: Tenable.io + Tenable.sc, ServiceNow (full suite)
• Pain: Can't demonstrate compliance, SLA breaches

IMPLEMENTATION:
• Duration: 14 weeks
• Cost: $280K (implementation + first year support)
• Team: 3 consultants, part-time

RESULTS AFTER 12 MONTHS:
Operational:
• Ownership ID time: 6 hours → 3 minutes
• Weekly tickets: 1,500 → 320

• Ticket response rate: 35% → 90%
• Critical MTTR: 60 days → 10 days
• High MTTR: 90 days → 25 days
• SLA compliance: 32% → 92%

Business:
• SOC 2 audit prep: 60 hours → 4 hours
• PCI assessment prep: 40 hours → 3 hours
• Security team time saved: 25 hours/week
• Avoided audit findings: Estimated 12
• Cyber insurance premium: Reduced 15% ($30K savings)

ROI CALCULATION:
Cost:
• Implementation: $220K
• Year 1 support: $60K
• Total: $280K

Savings:
• Security team: 25 hrs/wk × $85/hr × 52 = $110,500
• Audit prep: 93 hrs × $125/hr = $11,625
• Insurance premium: $30,000
• Avoided findings (risk): $50,000 (estimated)
• TOTAL SAVINGS: $202,125/year

Payback period: 1.4 years
3-year ROI: 116% ($606K savings / $280K investment)

CLIENT QUOTE:
"This integration transformed our vulnerability program from a compliance checkbox to a strategic capability. We went from constantly explaining to auditors why things weren't fixed to being able to demonstrate a mature, automated process."
- CISO

CASE STUDY 3: TECHNOLOGY STARTUP (300 employees)

CLIENT PROFILE:
• SaaS company, Series B funded
• 150 servers (AWS), 80 applications
• SOC 2 Type II for enterprise sales
• Had: Tenable.io, considering ServiceNow
• Pain: Rapid growth, no processes

IMPLEMENTATION:
• Duration: 8 weeks (fast-track)
• Cost: $160K (implementation + licenses + 6 months support)
• Team: 2 consultants, part-time

RESULTS AFTER 6 MONTHS:
Operational:
• Ownership ID time: N/A (new process) → 1 minute
• Weekly tickets: N/A → 85 (all properly routed)
• Ticket response rate: N/A → 88%
• Critical MTTR: N/A → 9 days
• SLA compliance: N/A → 90%

Business:
• SOC 2 initial audit: Passed with 0 findings (vuln section)
• Security team efficiency: 1 person handling program
• Lost deal recovery: 2 deals ($400K ARR) requiring SOC 2
• Investor confidence: Cited in Series C pitch

ROI CALCULATION:
Cost:
• Implementation: $90K
• ServiceNow + Tenable: $70K (year 1)
• Total: $160K

Value Created:
• Deals closed: $400K ARR × 30% margin = $120K
• SOC 2 achievement: Priceless for enterprise sales
• Security team productivity: 15 hrs/week saved
• QUANTIFIED VALUE: $120K+ (first year)

Payback period: 1.3 years (if only counting deals)
Strategic value: Enabled enterprise go-to-market

CLIENT QUOTE:
"As a startup, we needed to prove to enterprise customers that we had mature security processes. This integration gave us the foundation to achieve SOC 2 in our first attempt and win deals we would have otherwise lost."
- CTO

==========

SECTION 8: NEXT STEPS & ACTION PLAN

==========

IMMEDIATE ACTIONS (Week 1-2)

FOR CONSULTING FIRMS:

1. Assess internal capabilities
   - Do we have ServiceNow developers? (If no, hire or partner)
   - Do we have vulnerability management expertise?
   - Do we have relevant certifications?

2. Get certified
   - ServiceNow Certified System Administrator (CSA)
   - ServiceNow Certified Application Developer (CAD)
   - ServiceNow CIS - Vulnerability Response (if available)

3. Join partner programs
   - ServiceNow Partner Program (requires commitment)
   - Tenable Partner Program
   - Both offer co-marketing opportunities

4. Build demo environment
   - ServiceNow Personal Developer Instance (free)
   - Tenable demo/trial account
   - Build reference integration
   - Create demo scenarios

5. Develop marketing materials
   - One-page capability statement
   - Case study template (update as we get clients)
   - ROI calculator
   - Reference architecture diagrams

SHORT-TERM ACTIONS (Month 1-3)

1. Build reusable component library
   - Start with ownership mapping engine
   - Document design patterns
   - Create configuration guide
   - Version control in GitHub

2. Create service packages
   - "Quick Start" package definition
   - "Enterprise" package definition
   - Pricing calculator
   - SOW templates

3. Target first clients
   • Existing relationships with ServiceNow
   • Existing relationships with Tenable
   • Warm introductions through partners
   • Goal: 1-2 pilot clients at discounted rate

4. Execute first engagement
   • Deliver successfully
   • Document lessons learned
   • Create case study
   • Get testimonial and reference

5. Refine offering
   • Update components based on learnings
   • Adjust pricing if needed
   • Improve sales materials
   • Build out team if needed

MEDIUM-TERM ACTIONS (Month 4-12)

1. Scale delivery
   • Hire/train additional consultants
   • Standardize methodology
   • Build project templates
   • Create training program

2. Expand capabilities
   • Additional scanner integrations (Qualys, Rapid7)
   • Advanced analytics and ML
   • Cloud-specific enhancements
   • Container security workflows

3. Build brand
   • Speaking at conferences
   • Publishing thought leadership
   • Building community presence
   • Strategic partnerships

4. Product development
   • Package components as app
   • ServiceNow Store listing
   • Freemium/trial offering
   • Self-service configuration

5. Financial targets
   • Year 1: 5-8 clients, $800K-2M revenue
   • Build 3-6 month cash reserve
   • Invest in R&D (15% of revenue)

LONG-TERM VISION (Year 2-5)

YEAR 2:
• 15-20 clients
• $3M-5M revenue
• Team of 8-12 consultants
• Launch packaged app
• Expand to adjacent markets

YEAR 3:
• 30-40 clients
• $6M-10M revenue
• Team of 15-25
• International expansion
• Strategic partnerships

YEAR 4-5:
• 60-100 clients
• $12M-20M revenue
• Team of 30-50
• Consider acquisition opportunities
• Evaluate exit options

==========

CONCLUSION

==========

The Tenable + ServiceNow integration opportunity represents a high-margin,
scalable consulting business with multiple revenue streams:

KEY ADVANTAGES:
✓ Proven market demand (thousands of open ServiceNow positions)
✓ High consulting rates ($150-300/hour)
✓ Recurring revenue from platform resale and managed services
✓ Reusable components that improve margins over time
✓ Path to productization and exit

TYPICAL CLIENT ECONOMICS:

• Year 1 revenue: $250K-450K
• Year 1 margin: 50-55%
• Years 2+ revenue: $150K-250K/year
• Years 2+ margin: 55-65%

SUCCESS FACTORS:
1. ServiceNow development expertise (hire or build)
2. Vulnerability management domain knowledge
3. Reusable component library
4. Strong sales and marketing
5. Excellent delivery execution

RISKS TO MANAGE:
• Competition from larger consulting firms
• Platform vendor changes
• Keeping skills current
• Scaling delivery quality

The market opportunity is significant and growing. ServiceNow demand exceeds supply, and every enterprise needs better vulnerability management. By combining COTS platforms with custom integration expertise, consulting firms can build a profitable, sustainable business while creating valuable IP assets.

The time to act is now - the market is hot, rates are high, and the competitive landscape favors specialists with proven expertise.

==========

END OF DOCUMENT

==========