protiviti®
Global Business Consulting

World-Class Security Organization - Defined

How to deliver world-class security to your stakeholders

A world-class security organization is **nimble**, **efficient**, **self-improving**, **adaptive** and most importantly, **effective**. The characteristics below define selected characteristics of a world class security organization across applicable domains.

Domain	World-Class Characteristics	Benefits Achieved
IT Risk Management	• ERM integration • Real-time dashboards • User-level risk assessment • Leverage security info already collected • Use of FAIR or other robust risk assessment methodology	• Transform risk tracking to a decision support system • Efficient delivery of risk assessments
IT Compliance	• Automated collection, remediation and reporting of IT general controls (RPA) • Solid GRC platform; comprehensive control framework • Tight coupling of security, compliance and legal	• Less effort to maintain and report on compliance • Automated evidence collection; reduced effort for compliance activities
Third Party Risk Management	• Dashboard view of live vendor risk • Vendor risk platform/tool • Close integration with security, finance, legal, supply chain, etc. • Obtained data allows for better decision-making • FICO/Bitsight Score --> provide outside scores for third-party vendors • Automation of questionnaires and triage (define risk-level based on vendor; change in questions)	• Vendor Lifecycle Management from provision to deprovisioning to data destruction • Manage the risk that vendors bring vs. just get through the program • Prioritize risk over policy compliance • Concentrate resources on high-risk vendors • Make better sourcing decisions • Reduce administrative burden on vendor and internal teams (vendor can concentrate on giving good service)
Identity and Access Management	• User-centric (roles - look at the person vs. app) • Streamlined provisioning and deprovisioning • Cloud/CASB • MFA • Assignment of risk score to access levels (individual and aggregate) • Gamify to get users and managers to reduce risk score of access	• Improve authentication based on risk scoring • Revoke access based on certification status, observed activity and/or security events • Seamless to the user • Increased productivity • Reduced risk - identify issues before they happen
Privileged Identity Management	• Integrates and/or requires change control or problem management • Integration with MFA and session recording • Problem management • Automated one-time passwords • Automated tools to disable inactive privileged accounts • Abilities leveraged by system accounts	• Lower likelihood of privileged escalation • Reduced burden on admins • Increased service account management efficiency
Security Engineering and Tools Transformation	• Defined and referenceable architectural patterns • Self-service • ChatBots for policy questions • ChatBots for types / requirements	• Reallocation of personnel to more meaningful activity • Timely and detailed responses

INNOVATE. TRANSFORM. SUCCEED.

World-Class Security Organization - Defined

Domain	World-Class Characteristics	Benefits Achieved
DLP	• UEBA - Behavior heuristics • Advanced insider threat detection • Multi-layered approach (at rest, in motion, endpoint, CASB, etc.) • Leverages and feeds other verticals • AI identify patterns based on learning • Learning policy	• Reduced risk of data exfiltration • Efficient use of resources; ability to focus on advancement of capability
Vulnerability Management	• Automated scan schedules • Situational reporting aligned with owner and steward • RPA to create tickets, generate reports, etc. • Continuous scanning • Owner level reports • Automated config/patch deployment (Tachyon) • Integrated CI/CD remediation or delivery	• Resilient infrastructure delivered faster and with higher assurance • Increased efficiency/tighter integration with security and operations
Application Security	• Training • Immediate feedback via IDE plug-in • Static analysis (check-in and pipeline) • Automated dynamic analysis • Full automation of development and operations (DevOps) • AI/ML code analysis	• Speed to market (no roadblocks) • Less downtime / Fewer defects • Security is not a roadblock • Security baked into lifecycle
Disaster Recovery / Business Continuity Management	• Self-healing • Incorporating lessons learned • Integration with Incident Response, HR and IAM • Set policy to hot-hot / hot-warm • Automated call tree • Automated testing and regulatory documentation • Integration with third-party risk program • Integrated DDOS protection	• Trust in Disaster Recovery and Business Continuity working • Cost-effective
Event Management	• UEBA • Trends monitored, correlated and managed • Robust, fully functional SIEM • Use of AI for continuous analysis and improvement • Self-correcting / robust response • Level 1 / 2 automation (RPA)	• Stop events before they become issues • Proactively react before user-experience is disrupted • Reallocation of personnel to more meaningful activity • Reduced downtime, loss and disruption
Incident Response	• Functional team • Defined, repeatable process • Frequent training and drills; lessons learned incorporated • Metrics and measures • Event kicks off memory and disk snapshot (integrated) • Endpoints automatically quarantined	• Real-time response • Minimizing damage from event due to reacting quicker • Reducing breach timeline • Prevent data compromise (respond and contain) • Fewer mishandling of incidents due to automation (chain of custody is maintained)
eDiscovery and Forensics	• Alignment with Incident Response functions • Event kicks off memory and disk snapshot (integrated) • Endpoints automatically quarantined	• Support forensics as part of IR (not corporate investigations, etc.) • Shorter mean time to collect information
Threat Management	• Aggregate identity platform vulnerability and risk data • Automate the collection and correlation of data to allow personnel to provide analysis, and feed the machine learning capabilities • AI/ML associations to translate data into actionable intelligence • Data utilized for: Executive level threat indicators; intelligence briefs; immediate actions	• Actionable intelligence informs SOC, IR, leadership and infrastructure teams • Ability to measure and deliver response, reaction and relevancy

Protiviti.com/TechnologyConsulting **TechnologyConsulting@Protiviti.com** **TCblog.Protiviti.com**

protiviti®
Global Business Consulting