SOLUTION

Security Incident Response & Management

Discovering, Remediating and Preventing Security Incidents

A security incident can be the worst day of a company's business life. An organization's information and reputation can be harmed for years to come if a security incident is not discovered and remediated in time. **Quisitive's Security Incident Response & Management** team quickly assesses and remediates any damage the security incident could have caused and gets you back online as soon as possible. Whether it's a known compromise or a security breach, Quisitive will organize the technical response, engage your team, and guide the execution of incidence response measures. Our best-in-class security team will then help assess and improve your security posture to prepare against future attacks.

Preparation:

- Confirm understanding of suspected breach
- Ensure processes to prevent evidence loss
- Provide communication guidance for your teams

Detection & Analysis:

- Verify attack vector
- Identify full scope of the breach and information impact
- Perform event correlation, document the incident/facts surrounding
- Prioritize incident remediation areas

Containment, Eradication & Recovery:

- Preserve evidence & notify affected teams
- Identify the attacking host & a containment strategy
- Execute remediation strategy to eliminate the breach
- Recover systems to normal state.

Post-Incident Activity:

- Recover secondary systems
- Perform full environment security assessment
- Implement preventative measures to vulnerabilities
- Determine the evidence retention period
- Document lessons learned

Security & Compliance Management:

- Assessments and health checks
- Security coaching services
- Set-up and configuration of security tools
- Delivery of new and improved capabilities

Incident Areas

- Ransomware and phishing
- Compromised user accounts
- Data loss/ exfiltration
- Malware and Trojan viruses
- Lost or stolen devices

Response Team

- Security Office Governance Board
- Response Leadership Team
- Incident Response Manager
- Security Coach
- Technical Remediation Teams

Quisitive can help with:

REMEDIATION

- ✓ Servers (AD, SQL, Exchange, etc.)
- ✓ Azure Infrastructure (IAAS + PAAS)
- ✓ AD, Azure AD, AAD Connect, ADFS
- ✓ Identity Management Review
- ✓ Endpoint Review – all devices
- ✓ User Account & Passwords
- ✓ Environment Health Check
- ✓ M365 & O365 Security Remediation
- ✓ Client Communication Strategies
- ✓ "Do No Harm" Advisement
- ✓ Application Data Flow Review
- ✓ Custom App Authentication and Authorization Review
- ✓ Custom App Security Remediation
- ✓ Dynamics CRM Audit Data Investigation

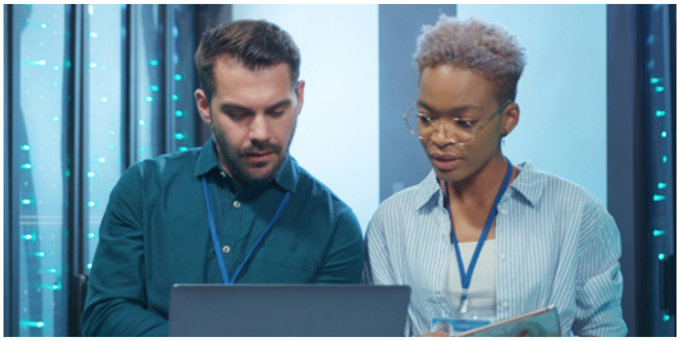
INCIDENT RESPONSE: REACTIVE

+

ONGOING SECURITY POSTURE

- ✓ M365 Security Assessment
- ✓ Azure Security Assessment
- ✓ Custom App Security Assessment
- ✓ Governance, Risk, Compliance
- ✓ Azure Sentinel & Security Center
- ✓ Microsoft Threat Protection
- ✓ M365 Defender & Azure Defender
- ✓ Identity Governance
- ✓ O365 External Sharing Guidance
- ✓ MS Info Protection & Data Loss Prevention
- ✓ MFA, Conditional Access, MCAS
- ✓ Advance Threat Analytics (On-Prem)
- ✓ Endpoint + Defender + AppGuard
- ✓ Compliance Center & Insider Risk
- ✓ Dynamics CRM Audit Enablement

SPYGLASS: PRO-ACTIVE IMPROVEMENT



Please note: Quisitive does not perform Security & Compliance Auditing (as separation of duties must be observed), Security Certification, Digital Forensics, Penetration (PEN) Testing, Application Security Testing & Hardening, Network Security Testing & Hardening, or Legal Representation & Evidence Collection. Should you need these, we can provide 3rd party vendor recommendations.