Cybersecurity is a pressing issue for virtually all industries and businesses of all sizes. Most organizations agree that they must be prepared for the inevitable. Those with a well-prepared incident response plan can respond to incidents more quickly, and minimize the potential liability that can arise from the breach. As part of that plan, outsourcing incident management is a viable security approach for many organizations.

Cylance® Consulting’s Incident Containment (Response) service provides the investigative support and direction an organization needs during an incident. Roadmaps for remediation will be planned and executed by our world-renowned experts to ensure the incident comes to a close.

**Service Overview**

Cylance Consulting will assist your organization with responding to a suspected security incident. Our approach is to stop the active threat while applying proprietary tools and processes to quickly diagnose the environment and remedy the situation. Activities include:

**Incident Containment**
- Investigative support and direction
- Malware, forensic, and log analysis
- Remediation planning and assistance
- Regular status reporting and project management-related activities
- Reporting and/or presentations associated with findings and recommendations

**Forensics Investigation**
- Determine the investigation scope
- Create an investigative plan
- Conduct forensic acquisition of electronic data
- Adhere to strict chain-of-custody procedures
- Analyze acquired data
- Report and/or present on findings and recommendations

**Benefits:**
- Containment achieved within days, not months
- More resources, specialized services, managerial skills, and an in-depth perspective on threats and how to remediate them
- Access to malware experts who can add perspective in making decisions and reaching agreements with internal teams
- Proprietary tools and proven methodologies to respond faster and more accurately
- A detailed incident scope, which can be determined with confidence
- Strategic malware, forensic, and log analysis reporting educates internal teams

64% of respondents say the volume of cybersecurity incidents and severity of security incidents have increased.

*Source: 2018 Cyber Resilient Organizations, Ponemon Institute*
Deliverables
Cylance Consulting will furnish a comprehensive report detailing:
• Testing results via a graphic summary
• A strategic remediation roadmap
• Our findings, including:
  • Name and details of threats discovered
  • Vulnerable host/IP
  • Severity of vulnerability
  • Detailed recommendations
  • Priorities including assigned owners

Ensure your organization has access to experienced IR experts before you are faced with a security incident. Contact Cylance Consulting or your technology provider to discuss your incident response needs.