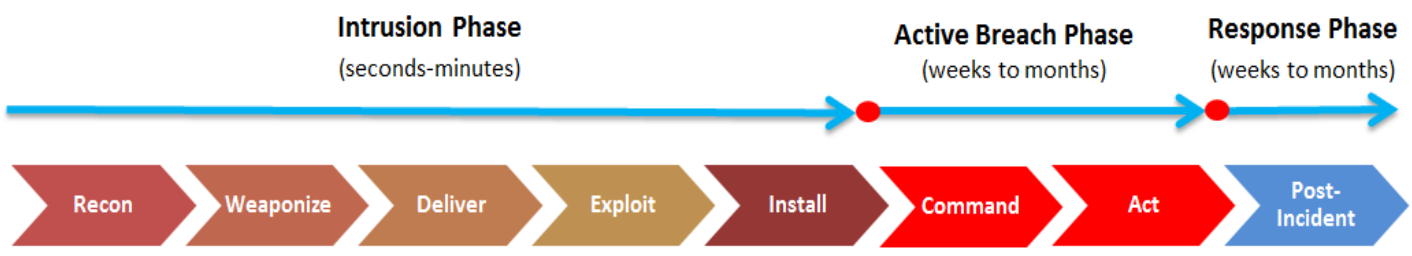
WILEY Security Program Overview

This document provides an overview of the security program at John Wiley & Sons, Inc.

WILEY SECURITY OPERATIONS CENTER (W-SOC) CAPABILITIES

Central to global security operations is the Wiley Security Operations Center (W-SOC). The primary goal of the security operations team is to prevent or detect breaches as early as possible in the Cyber Kill Chain ®:



Cyber Kill Chain® Model
Developed by Lockheed Martin

W-SOC is a 24x7x365 operation responsible for detection, triage, and incident response procedures.

W-SOC security analysts prevent and/or detect breaches using next-gen technologies that create multiple security layers for protection of infrastructure and data. This includes, but is not limited to:

- DDOS and web application firewalls
- Perimeter firewalls
- Intrusion detection systems/ intrusion prevention systems
- Multiple vulnerability scanning tools
- Signature and behavioral based analytics at the host and network layers
- Cloud-based proxy
- DNS Security
- Advanced Email Threat Protection
- Threat intelligence & SIEM
- Layer 7 firewalls (deep content inspection, egress traffic monitoring)

The W-SOC team employs a minimum of three SANS GIAC certified staff who serve as SME within the larger global security operations team.

NIST CSF: CYBERSECURITY FRAMEWORK

Wiley's security policies, standards, procedures and guidelines follow the National Institute of Standards & Technology Cybersecurity Framework (NIST CSF). The NIST CSF serves as a policy framework of computer security guidance for how organizations can assess and improve their ability to prevent, detect, and respond to attacks and security incidents.

Wiley's security program follows the NIST 800-61standard (*Computer Security Incident Handling Guide*) for its Incident Response Plan.

GOVERNANCE, RISK & COMPLIANCE

Wiley maintains an enterprise-wide IT Governance, Risk, and Compliance (GRC) program that ensures availability, integrity, and confidentiality of Wiley's information assets, including any customer data under the company's custody. Additionally, the GRC team serves as independent reviewers of risks for all other operational areas.

Information Technology Sarbanes-Oxley (SOX) Compliance Program:
Wiley is subject to the Sarbanes-Oxley Act. As such, internal and external auditors routinely assess the network and data security via testing of ITGC (IT General Controls), and ITAC (IT Application Controls).

Payment Card Industry (PCI) Compliance:
Wiley is a Level 3 PCI compliant merchant.

Privacy Shield and GDPR:
Wiley has submitted its Privacy Shield certification application with the Department of Commerce, approval pending, and has a program in place to address requirements for GDPR.

Wiley is a TRUSTe certified organization

FOR MORE INFORMATION CONTACT

Reginald Zamora
CISO & VP - Information Security & Compliance
rzamora@wiley.com