SCHNEIDER DOWNS

Big Thinking. Personal Focus.

Cybersecurity Services

DIGITAL FORENSICS AND INCIDENT RESPONSE

In today's cybersecurity climate, breaches are often not a matter of if, but when. Schneider Downs' team of Digital Forensics and Incident Response experts have experience helping clients respond to a multitude of threat vectors and attack types. We work with you to determine the exact factors that led to the breach, assist you in recovery, and develop lessons learned to better mitigate these types of events down the road. This process allows for restoration of faith that your systems will be hardened against future attacks and preserve business relationships and public trust.

Don't wait until it's too late. Schneider Downs experts can be engaged ahead of a breach, through a retainer contract or during emergency situations as needed.

INCIDENT RESPONSE PROCESS

RECOVERY AND REMEDIATION

Recovery and remediation is a major component of the Schneider Downs Incident Response process. Our team has the expertise to recover major disruptions to IT systems and help your organization:

1. Form and identify the remediation team;
2. Determine the timing and extent of remediation activities needed;
3. Develop and implement remediation posturing actions during the incident (password resets, two-factor deployments, etc.);
4. Develop and implement containment actions;
5. Develop and implement an eradication action plan;
6. Develop strategic recommendations for safe recovery;
7. Document and report on lessons learned

FORENSIC ANALYSIS

From a forensics standpoint, our trained experts use the most advanced technology and analysis methods to:

1. Ensure the incident or malware is contained and unable to breach additional systems
2. Provide detailed analysis on production systems for malware or threat actor persistence
3. Perform detailed forensic analysis of suspected compromised hosts
4. Review all event logs and provide a detailed report on current auditing procedures
5. Assess all network traffic and perform detailed threat analysis for potential malware command and control communications
6. Review all Intrusion Detection Systems (IDS) or Intrusion Prevention System (IPS) alerts for malicious activity
7. Perform static and dynamic malware analysis on discovered payloads executed on victim machines

8. Provide a detailed list of recommended remediation procedures and long term cybersecurity enhancements
9. Provide a detailed report on all discoveries

OTHER SERVICES AND CAPABILITIES

In addition to the services above, our team also offers a myriad of other services including:

- Cloud Security Strategy
- Endpoint Hardening Consulting
- Enterprise Information Security Program Review and Consultation
- External Footprint Analysis
- Firewall Configuration Review
- Indicator of Compromise Assessment
- Information Security Program Maturity Assessments
- Infrastructure Assessments
- Intrusion Prevention/Detection Review
- MS Office 365 Security Assessment
- Network Device Hardening & Configuration Assessments
- Phishing Assessments
- Physical Security Assessments
- Ransomware Prevention
- Sensitive Data Discovery Assessments
- Vulnerability Analysis
- Wireless Security Assessments

SOFTWARE SOLUTIONS

Schneider Downs is an authorized reseller for a number of software solutions, including Carbon Black®, Mimecast®, Guardicore and Sophos.

WHY SCHNEIDER DOWNS?

Schneider Downs can help your organization be better prepared. We offer a comprehensive set of information technology security services, including network penetration assessments, network vulnerability assessments, web application security testing and IT security maturity assessments. Our expert team includes application configuration specialists, implementation consultants and certified information system auditors who can assist your organization with an objective assessment, identify crucial information and key security risks, and assist with the implementation of industry best-practice security standards to mitigate these risks. For more information visit our website at www.schneiderdowns.com/cybersecurity or contact us at cybersecurity@schneiderdowns.com.

EXPERIENCING OR SUSPECT A NETWORK INCIDENT?

Contact the Schneider Downs Incident Response Team 24x7x365 at 1-800-993-8937.

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

www.schneiderdowns.com

TAX

AUDIT AND ASSURANCE

CONSULTING

WEALTH MANAGEMENT

PITTSBURGH
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

COLUMBUS
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

WASHINGTON, D.C.
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003