


The logo for SpearTip, featuring the word "SPEARTIP" in a bold, sans-serif font. The letter "A" is replaced by a stylized blue triangle pointing upwards.

A company of  ZURICH®

Incident Response Engagement

SpearTip engages in ransomware events daily, helping organizations of varying sizes and within any industry minimize data loss and resume operations as soon as possible. Our experienced team has been leading incident response (IR) engagements since 2005 and will help guide you through the technical aspects of the response.

The accompanying information provides insight into how your team should respond to an incident and the typical stages of an IR engagement with our team as your IT operations are restored and a forensics investigation is conducted.



Breach Response
833.997.7327

Emergency: breachresponse@speartip.com
Non-Emergency: info@speartip.com

ISOLATE IMPACTED SYSTEMS

As soon as malicious activity is detected in your environment, isolate those affected systems from the internet and the rest of your network to prevent any further spread. SpearTip will need access to the impacted systems to determine exactly what occurred before they are restored to a clean state or rebuilt from available backups. **Failure to preserve evidence could make the situation worse.** If in doubt about restoring a system, call the SOC.

CHANGE PASSWORDS

In the vast majority of cyber incidents, the threat actor has been able to attain password dumps from your environment. **It is critical that you *immediately* reset all passwords within Active Directory and any remote access solution (VPNs, RMMs), including any service, local administrator, or domain administrator accounts.** Failure to do this could allow the threat actor to return and further attack the environment.

DO NOT ENABLE RDP OR UNPATCHED VPNs

In a significant amount of attacks, a vulnerable remote access solution is leveraged. **It is critical that you do not enable public internet access via remote desktop protocol (RDP) on any server or allow any unpatched VPNs back online.** RDP should not be reenabled at any point, and a VPN should be implemented instead. All VPNs should be fully patched, multifactor authentication enabled, and credentials reset prior to bringing them online.

CONTACT VITAL STAKEHOLDERS: INSURANCE & CYBER SECURITY

Do not attempt to resolve a significant cybersecurity incident on your own. If you have a cyber insurance provider, contact your representative immediately to report the incident. They should then assist you in working with a provider of IR services to limit the damage, prevent lateral spread, and get your business back up and running as soon as possible.



DATA BREACH INVESTIGATION

During an investigation, we analyze data and provide guidance on what to do next. We find retrievable data, exhaust available response methods, and work to get your organization up and running. Our SOC is staffed 24/7, working in a continuous investigative cycle, ready to respond to events at a moment's notice.

SHADOWSPEAR or CLOUD MONITORING DEPLOYMENT

The most critical step in the recovery process is to ensure the environment is protected from further malicious activity and any threat actor is removed. We do this by deploying ShadowSpear, our monitoring and remediation toolset, to laptops, desktops, servers, and/or application tenants for 45 days.

DECRYPTION ASSISTANCE (OPTIONAL)

We can go to work on your behalf to gain access to the decryptor to safely recover any assets accessed or manipulated by a threat actor. Once we have the decryptor, our team tests it to ensure it is safe and works as it should. As this is verified, we continue to assist your team in completing the data decryption process as needed.

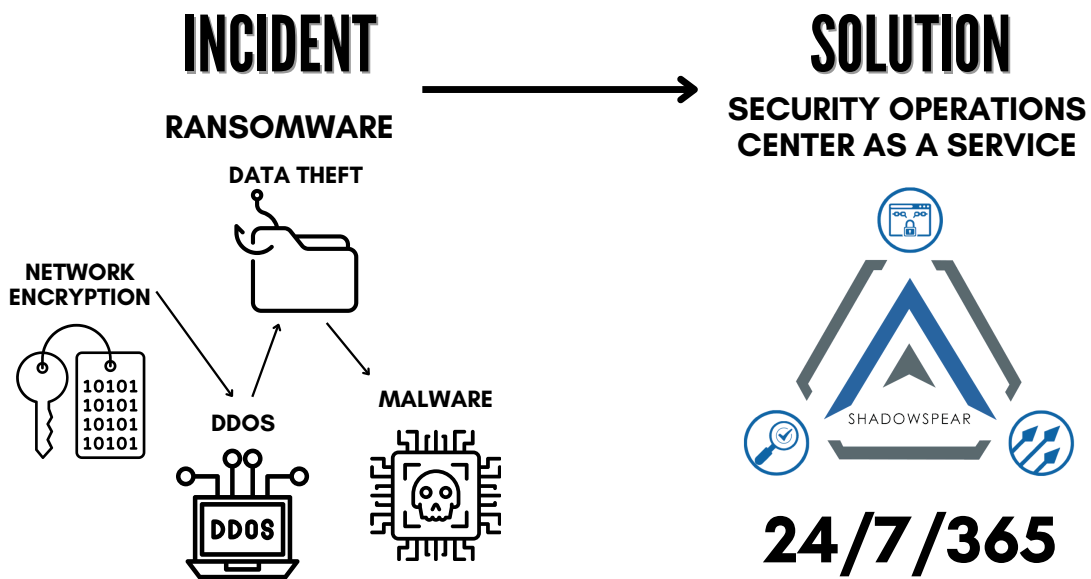
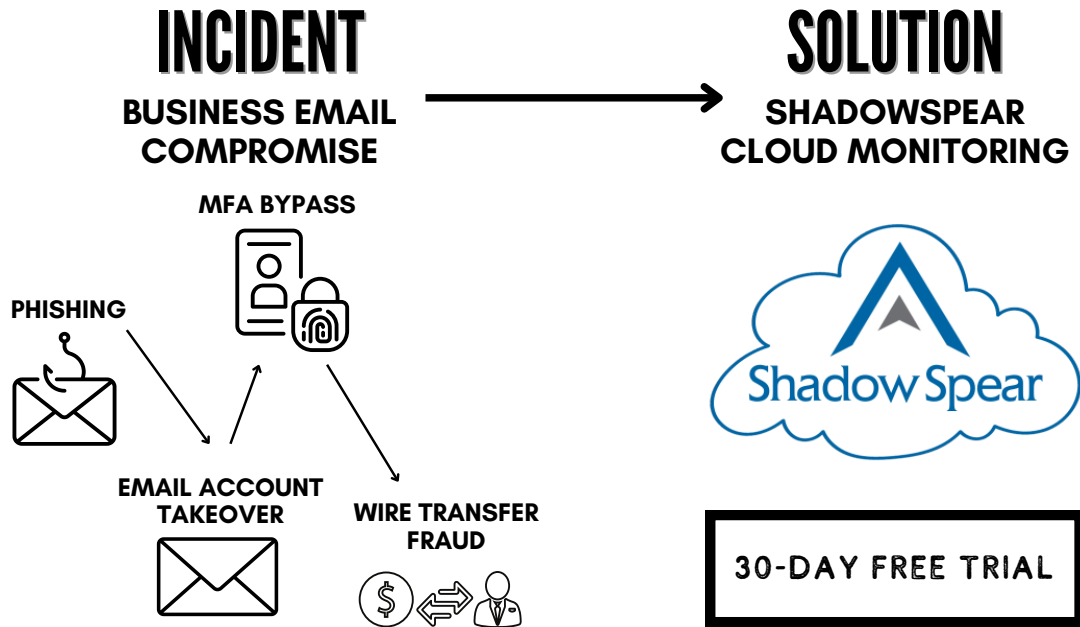
DIGITAL FORENSICS

Our digital forensics services start with proper gathering, handling, and cataloging of information that can be used to understand the incident's cause or help in court. We help with evidence discovery, forensic analysis, reconstruction, and courtroom strategy.



Solutions Designed To Address Today's Threats

Our ShadowSpear Platform solutions help prevent various cyber threats.



Breach Response
833.997.7327

Emergency: breachresponse@speartip.com
Non-Emergency: info@speartip.com

What does a typical engagement look like?

Below is what an incident response engagement with our team might look like.



This is a general description of certain types of managed security services, including incident response, continuous security monitoring, advisory, and/or other risk engineering or risk management services provided by Zurich Resilience Solutions, which is part of the Commercial Insurance business of Zurich Insurance Group and does not represent or alter any insurance policy or service agreement. Such services are provided to qualified customers by affiliates of Zurich Insurance Company Ltd, including but not limited to SpearTip, LLC, 1714 Deer Tracks Trail Suite 150, Saint Louis, MO 63131, USA, The Zurich Services Corporation, 1299 Zurich Way, Schaumburg, IL 60196, USA, and Zurich American Insurance Company, 1299 Zurich Way, Schaumburg, IL 60196, USA. The opinions expressed herein are those of SpearTip, LLC as of the date of the release and are subject to change without notice. This document has been produced solely for informational purposes. All information contained in this document has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Company Ltd or any of its affiliated companies (collectively, Zurich Insurance Group) as to their accuracy or completeness. This document is not intended to be legal, underwriting, financial, investment or any other type of professional advice. Zurich Insurance Group disclaims any and all liability whatsoever resulting from the use of or reliance upon this document. Nothing express or implied in this document is intended to create legal relations between the reader and any member of Zurich Insurance Group. Certain statements in this document are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by numerous unforeseeable factors. The subject matter of this document is also not tied to any specific service offering or an insurance product nor will it ensure coverage under any insurance policy. No member of Zurich Insurance Group accepts any liability for any loss arising from the use or distribution of this document. This document does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction. In the United States, managed security services are provided by SpearTip, LLC and risk engineering and risk management services are provided by The Zurich Services Corporation.

