WE SAFELY ENABLE BUSINESS

Incident Response

The Computer Security Incident Response Team (CSIRT) is an elite Pan-European team within SecureLink that provides consulting, incident management and technical advice to help customers handle a security incident from initial detection to closure.

Introduction

Media reports of large data breaches used to be few and far between, hidden away inside the pages of the tech section of the news, or dedicated industry news sources. The reality now, is that breaches are mainstream news. With incidents on the increase, your company's reputation could be on the line.

The key to mitigating the impact of any IT security incident, is the reaction time between detection and response. Many companies lack the infrastructure needed to react in a quick and secure manner. Securelink SecureRespond services allow any company to react 24/7 to malicious cyber threats. Enabling customers to complement existing resources with world class expertise, to safely enable their business.

Once a breach is detected, however that happens, the further challenge then is how to respond. You typically require:

• **Expertise.** Experience and skills make an impact especially in response to critical cybersecurity incidents. SecureLink's CSIRT continuously refine and update our methodologies and techniques. This allows our teams to handle security incidents with confidence and in an efficient manner. Using our combined knowledge to identify, contain, eradicate and recover from a range incidents.

• **Reliability.** With ever increasing regulations such as GDPR and the emerging market of Cybersecurity Insurance, requiring assessment and reporting of incidents faster than ever before, a solid partner who can deliver on providing the expertise required time after time is crucial. In what is often most companies' greatest hour of need, you require someone you can trust.

• **Preparation.** Pro-active services help you to plan, prepare, train and test your people, processes and technology so that when incidents do happen, the organisation is ready and confident, in tried and tested methodologies used to manage the response.

The SecureLink CSIRT

The SecureLink CSIRT is an Pan-European team within SecureLink Group, Europe's largest independent cybersecurity and Managed Security Service provider. The CSIRT can be deployed to provide expert consulting, incident management and technical advice to help you handle a security incident end-to-end from the initial detection to closure.

We will help you manage an entire incident, from a simple breach of policy to an estate-wide compromise working as a key part of your organisation's incident response plan and as a colleague within your own incident response team.

The CSIRT follow the principles of the 'Association of Chief Police Officers' (ACPO) Good Practice Guide for Computer-based Electronic Evidence' for all aspects of evidence management, regardless of criminal circumstances or law enforcement agency involvement.

WE SAFELY ENABLE BUSINESS

Working with us

Our CSIRT provides all of the key components for a world class incident response function:

Technical Experience

It is important to have experienced responders who are comfortable and confident in dealing with what are often high pressure situations. SecureLink's CSIRT members have worked with some of the world's largest enterprises and responded to some of the most devastating and high profile cyber-attacks of recent times, including Petya and WannaCry.

Qualifications

All personnel working on incident response activities are certified to the CREST Registered Intrusion Analyst level at a minimum or equivalent certification/ experience. Experience and skill-sets, backed up by internationally recognised standards and methodologies (including a CREST certified methodology) give you the assurance that you are in good hands.

Knowledge

SecureLink know your business. Our incident response retainer services include an on-boarding risk assessment workshop to ensure our team have a detailed overview of the current position, to gain maximum insight before a response is required.

Retainer

It is important that you have a guarantee of quality skills when you need them most; preparation is key. The SecureLink CSIRT are available on retainer basis 24x7, 365 days a year with a guaranteed remote and responder to site SLA. Our retainer services are designed so that unused retained hours can be utilised for pro-active work such as testing, training and process review.*

*Depending on service level purchased.

Containment

With outbreaks of ransomware and other malicious malware threatening industries of all types, containment is vital. With SecureLink's strong partnership with leading threat detection and containment product vendors alongside a combination of in-house and commercial toolsets honed across years of IR work, we look to ensure that if your defences have been breached, the threat is prevented from escalation and damage is limited to a minimum.

Intelligence

We collect Indicators of Compromise (IOCs) from every incident response engagement. SecureLink have access to global threat intelligence from commercial and open sources, and our CSIRT team are closely linked to the SecureLink Cyber Defense Centre (CDC). The two-way sharing of information between the CSIRT and CDC, fully utilises the Cyber Threat Intelligence we have at our disposal, allowing us to better advise on preparing for future incidents and to provide focused context around an incident or series of incidents.

Summary:

- Delivers high quality incident response when you need it (on-demand or on a retainer basis)
- Develops your internal skills, documentation and processes to allow you to be ready for a broad array of incidents
- Incorporates a vast wealth of experience, cyber threat intelligence and a passion for quality service and customer satisfaction

About SecureLink

We're specialists in cybersecurity. It's our focus every hour of the day, every day of the year. That's why we're among the best – if not the best – in the world at what we do. But true cybersecurity isn't just about protection. It's about enabling, too. It's about empowering businesses by allowing them to safely embrace innovation, efficiency and collaboration. True cybersecurity is about adding value by building trust and making life easier for our customers.

This is why, at the heart of SecureLink, is a philosophy that extends beyond the supply of advanced technology. It's a philosophy that demands a complete understanding of your needs, so that we are more than just a supplier: we supply appropriate technology – technology that's right for your business environment and strategy for growth; technology that protects you not only now, but always, as your needs and circumstances change. Only then can you have and maintain the levels of trust and confidence you need to succeed in today's digitally-driven business world.

© SecureLink. All rights reserved worldwide.