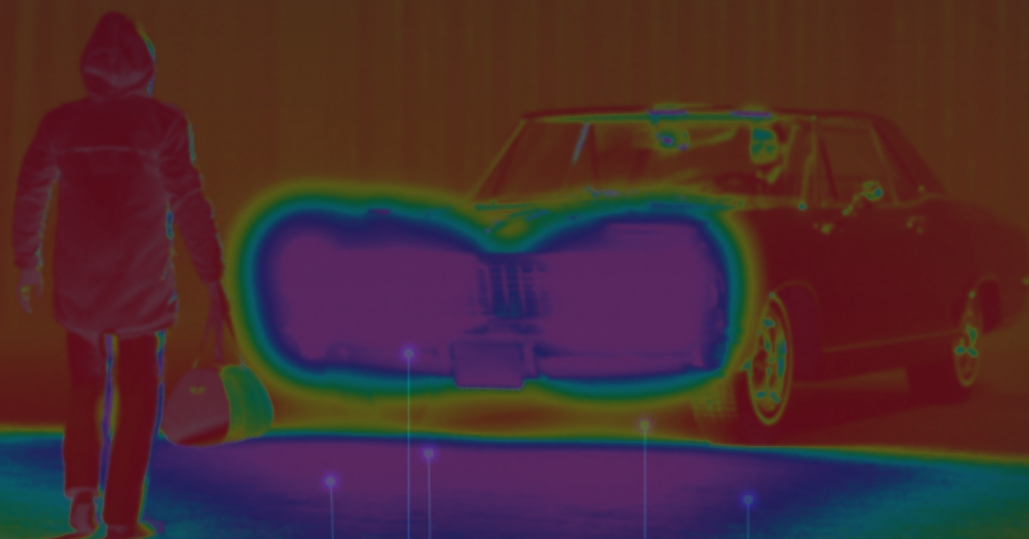


E-BOOK

# Facing Ransomware Head On

## Building the Resilience You Need



**GUIDEPOINT**  
SECURITY

# Bringing **Calm** to the Chaos



Of course you remember the **iconic phone call scene in *Taken***. Liam Neeson's character has been told that his daughter is being held for ransom. Does he panic? No. Instead, he stays calm, and applies his very specific expertise and skill set.

**"...I do have a very particular set of skills, skills I have acquired over a very long career, skills that make me a nightmare for people like you."**

That's the attitude you need on your side to confront ransomware gangs. Cyber insurance may not be enough. But what you can get is expertise.

GuidePoint Security has a very particular set of skills... skills we have acquired over a very long career.

Skills that can give peace of mind in an ever-changing security landscape.

An unfortunate truth in today's security landscape is that ransomware attacks are now more prevalent than they ever have been. Given the number of ransomware attacks, most cyber insurance companies are becoming more cautious when underwriting policies. While they still offer coverage, it might come with very high premiums, depending on your security posture.



The good news is that GuidePoint Security can help you build resilience in the face of these attacks, with strategies that can:

### **SAVE YOU MONEY**

---

by leveraging existing toolsets and data sources along with supplemental solutions.

### **SAVE YOU TIME**

---

by using a process that goes beyond industry standard Incident Response frameworks.

...and in the end, **assists with maintaining your brand's reputation.**

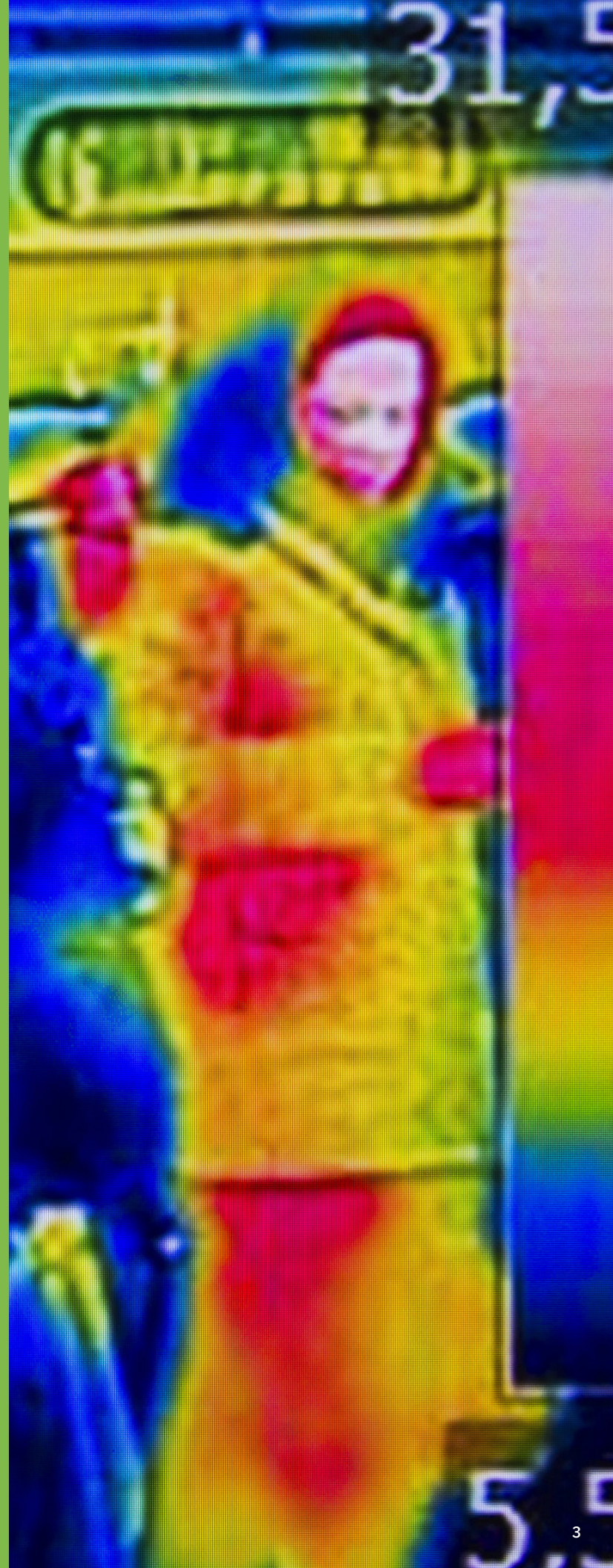
GuidePoint Security's team of practitioners have a wide range of industry-standard certifications from SANS, ISC2, and Offensive Security, to name a few, and bring to bear core knowledge and the capabilities of our resources to perform the investigation. We also have extensive experience with the pertinent legal processes and policy requirements.

### **"I WILL FIND YOU": INCIDENT RESPONSE ENGAGEMENT METHODOLOGY**

---

We leverage your existing toolsets and data sources in conjunction with supplemental solutions that can be deployed for environmental visibility. With full visibility across network, endpoint, logs and other data sources, our team can obtain current and historical situational awareness. This gives us an all-inclusive picture of any potential threats in your environment.

Then we develop a comprehensive remediation strategy, which includes tactical and strategic recommendations to remove threat actors, and establish a baseline to address future threats.





# “I do have are a very particular set of skills”

## Core Competencies

We have dedicated Incident Response practitioners who are experienced in a wide variety of industry standard tools and solutions. This provides the required visibility across your network, endpoints, and other systems, ensuring an efficient and comprehensive investigation.

### THE CORE KNOWLEDGE AREAS AND CAPABILITIES WE USE TO PERFORM THE INVESTIGATION INCLUDE

- ✓ Network traffic analysis
- ✓ Log collection and review
- ✓ Host analysis and mass triage of forensic artifacts
- ✓ Malware analysis and reverse engineering
- ✓ Forensic disk imaging, memory acquisition and review
- ✓ Current and advanced threat expertise
- ✓ IR methodology and response techniques

### THE DOUBLE THREAT

#### A Particular Set of Skills + Well-Defined Engagement Structure

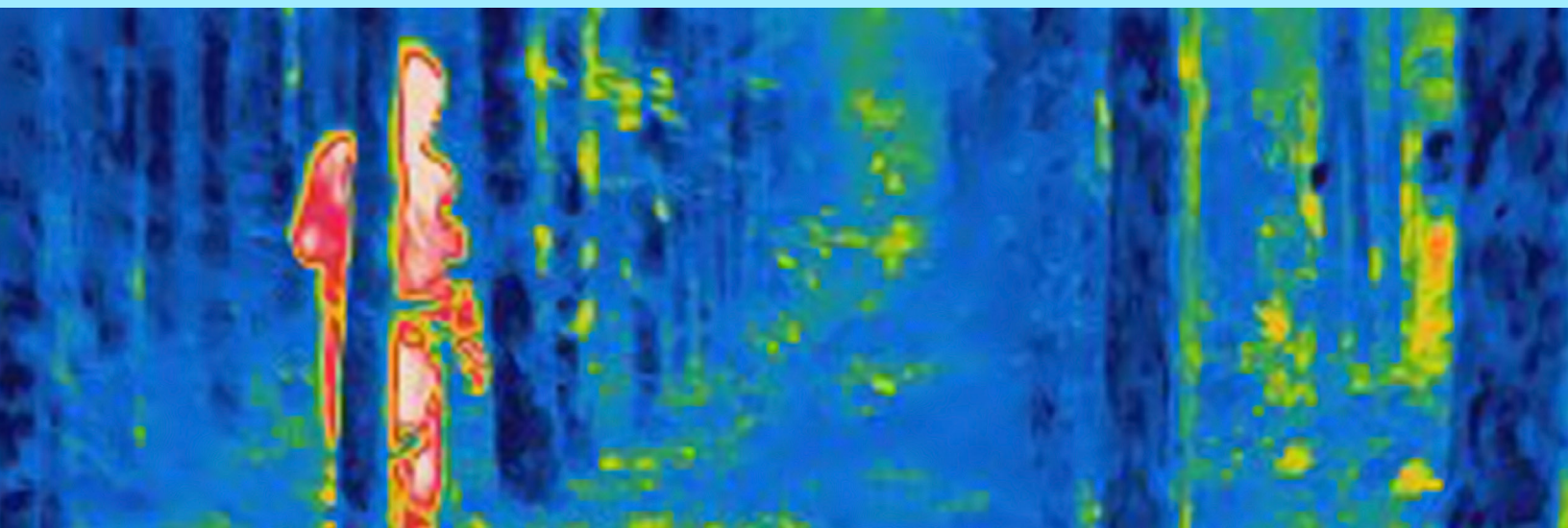
Our process comprises preparation, identification, containment, eradication and recovery phases aligned with our incident response methodology.

Our IR team develops an engagement plan specific to your environment and requirements. The engagement plan includes detailing tasks, deliverables, methods of communication, status cadence and more. This way, we can ensure effective communication, collaboration, and direction throughout the entire engagement.

### COVER UP, LAWYER UP

#### Cyber Insurance & Legal Counsel

We work closely with several cyber insurance providers/carriers and third-party legal counsel in delivering incident response services. We have experience with the legal processes, policy requirements, and other details that ensure a smooth and collaborative engagement with your organization and third parties.



# Who the Good Guys Are Certifications & Bios



The team members responding to the incident come from a variety of backgrounds. They have extensive industry experience and carry several industry standard certifications: SANS, ISC2, Offensive Security, as well as from cloud service providers and many others. If you are interested in individual bios from team members, we are happy to provide them.

Start building resilience today. Check out GuidePoint Security's comprehensive services on [Incident Response and Threat Intelligence](#). Or feel free to [contact us](#).



# GUIDEPOINT

## SECURITY



2201 Cooperative Way, Suite 225, Herndon, VA 20171  
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132  
07.2022