The Impact of Dragonfly Malware on Industrial Control Systems

By Created by:Nell Nelson

Download File

The Impact of Dragonfly Malware on Industrial Control Systems (PDF, 1.45MB)Published: 22 Jan, 2016

Dragonfly malware infected hundreds of business computers in an often successful attempt to collect information on industrial control systems across the United States and Europe. The attack was performed in an orchestrated manner over an extended period of time and used infection methods that were difficult to detect and thwart. The malware collected information vital to the operation of the impacted systems across the energy and pharmaceutical sectors. This abstract will explore the impact of Dragonfly Malware on systems used for automated industrial control. The content will explain the manner in which Dragonfly infiltrated business systems in both Europe and the United States, how it was discovered, and the immediate and future impact of the malware on infected systems and on the ICS industry. This paper will also discuss ways in which the industry can safeguard itself against future attacks similar to the Dragonfly malware effort.

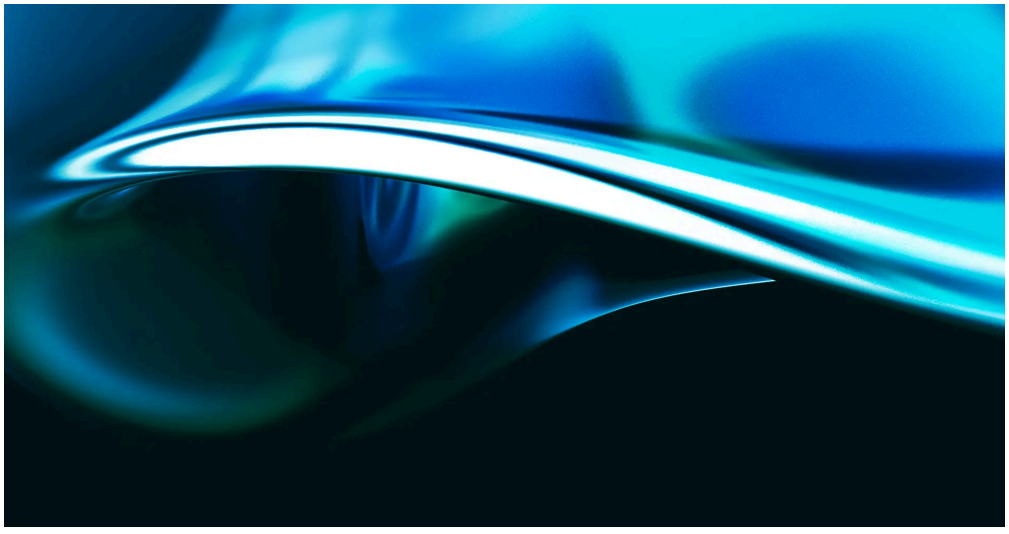
Additional resources

Related courses

- Slide 1 of 7

ICS515: ICS Visibility, Detection, and Response

ICS515Industrial Control Systems Security



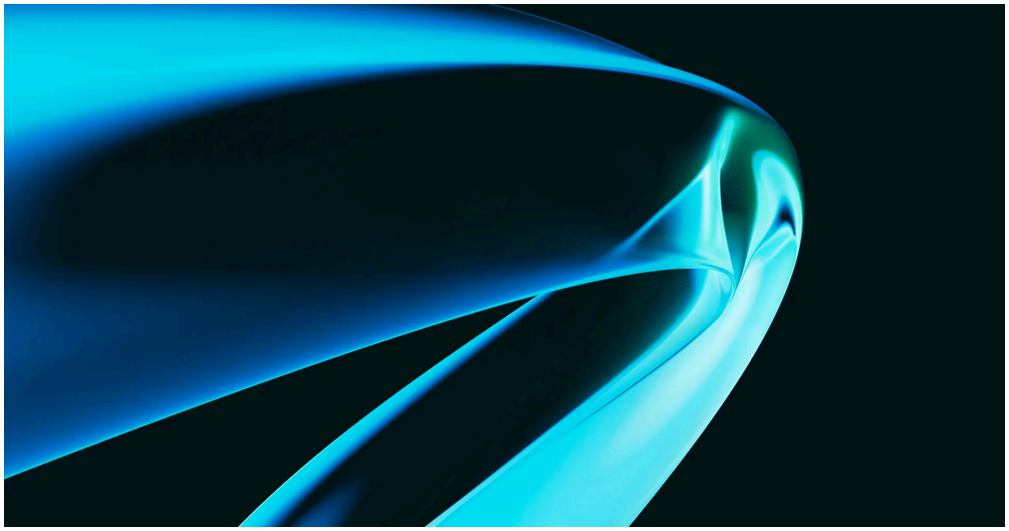
- GIAC Response and Industrial Defense (GRID)
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 22 Hands-On Labs

View course detailsRegister

- Slide 2 of 7

ICS418: ICS Security Essentials for Leaders

ICS418Industrial Control Systems Security



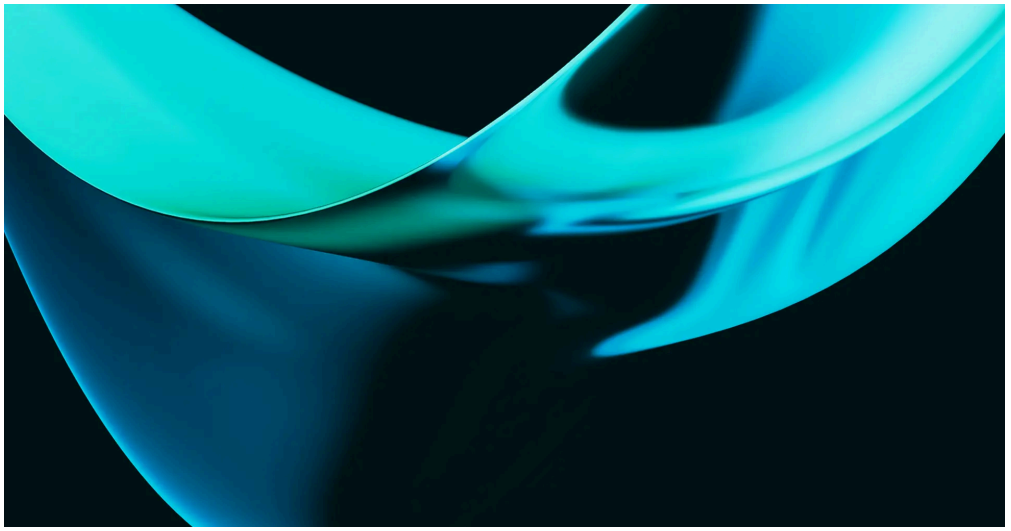
- 12 CPEs / 12 Hours (Self-Paced)
- Labs: 12 Hands-On Labs

View course detailsRegister

- Slide 3 of 7

ICS613: ICS/OT Penetration Testing & Assessments

ICS613Industrial Control Systems Security



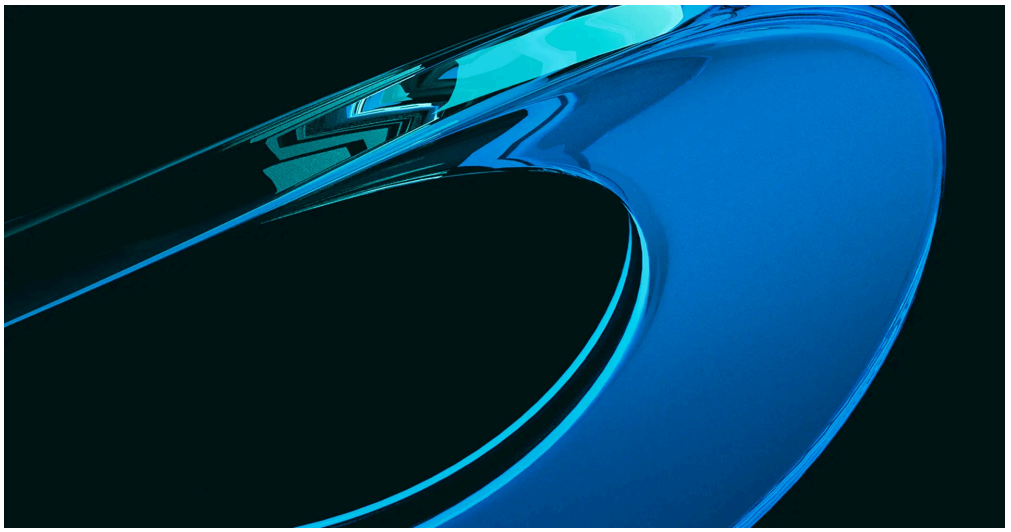
- 5 Days (Instructor-Led)
- 30 CPEs / 30 Hours
- Labs: 27 Hands-On Labs

View course detailsRegister

- Slide 4 of 7

ICS456: Essentials for NERC Critical Infrastructure Protection

ICS456Industrial Control Systems Security



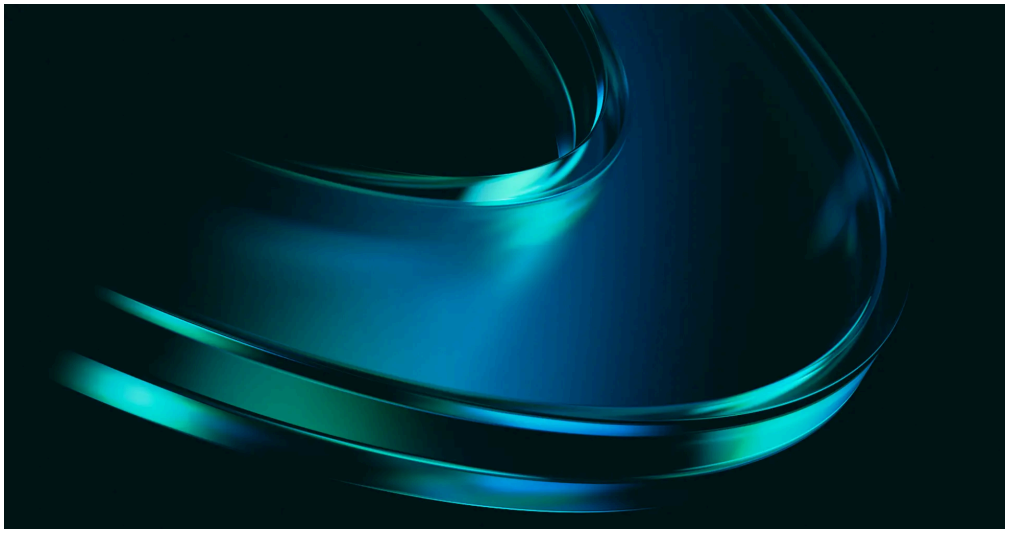
- GIAC Critical Infrastructure Protection (GCIP)
- 5 Days (Instructor-Led)
- 31 CPEs / 31 Hours (Self-Paced)
- Labs: 23 Hands-On Labs

View course detailsRegister

- Slide 5 of 7

ICS310: ICS Cybersecurity Foundations

ICS310Industrial Control Systems Security



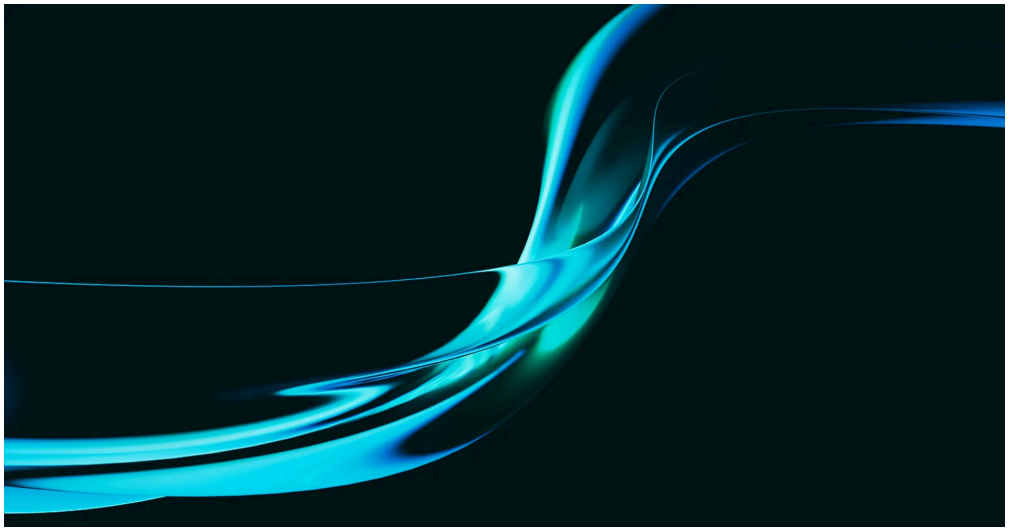
- 12 CPEs / 12 Hours (Self-Paced)
- Labs: 3 Hands-On Labs

View course detailsRegister

- Slide 6 of 7

ICS410: ICS/SCADA Security Essentials

ICS410Industrial Control Systems Security



- GIAC Global Industrial Cyber Security Professional (GICSP)
- 6 Days (Instructor-Led)
- 36 CPEs / 36 Hours (Self-Paced)
- Labs: 15 Hands-On Labs

View course detailsRegister

- Slide 7 of 7

ICS612: ICS Cybersecurity In-Depth

ICS612Industrial Control Systems Security

- 5 Days (Instructor-Led)
- 30 CPEs / 30 Hours
- Labs: 31 Hands-On Labs

View course detailsRegister
