# The New Era of Cyber Threats

## The Shift to Self-Learning, Self-Defending Networks

Georgiana Wagemann

Director of Sales, Darktrace

# Evolving Threats in a New Business Landscape

DARKTRACE

- Outsourced IT, SaaS, cloud, virtual, supply chain, IoT
- Not just data breaches and defaced websites
- ‘Trust attacks’ are silent and stealthy
- AI attacks are emerging, leading to highly customized campaigns
- Machine on machine attacks

# Machine Learning is Hard to Get Right

DARKTRACE

- No two networks are alike
- Needs to work without customer configuration or tuning of models
- Needs to support teams with varying security and math skills
- Must deliver value immediately but keep learning and adapting as it goes
- Cannot rely on training sets of data

# Insider Threat

- 28% of attacks involve insiders
- People do make mistakes – human error caused one in 5 breaches
- Privileged access users also pose a risk
- Social engineering becoming more sophisticated

# Low and Slow vs. Machine Speed

- Stealthy attacks incredibly difficult to detect with traditional security tools
- Machine-speed attacks on the rise
- Requires action in minutes
- Ransomware is the most common type of malicious software – present in 39% of malware cases

# Cloud

- IT and security teams have less visibility
- Expanded attack surface
- Ease of spinning up a cloud instance allows developers to rapidly bypass the security team
- New threat vectors

# Internet of Things

- IoT devices are transforming industries, our homes, our cities, and our offices
- Millions of endpoints and vast quantities of data
- Security not built into IoT devices
- Introducing increasing complexity

# Industrial Control Systems

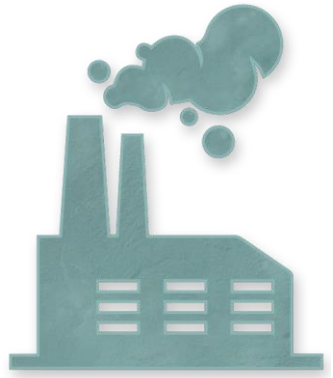
DARKTRACE

- Risks to ICS and SCADA increasing
- Beyond security, issue of safety
- Regular and consistent network activity
- Tuning the AI to a higher degree of sensitivity

# Cyber AI Platform

DARKTRACE

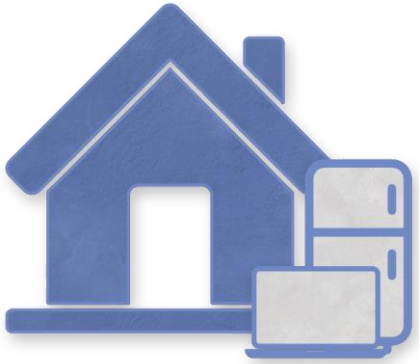
Enterprise



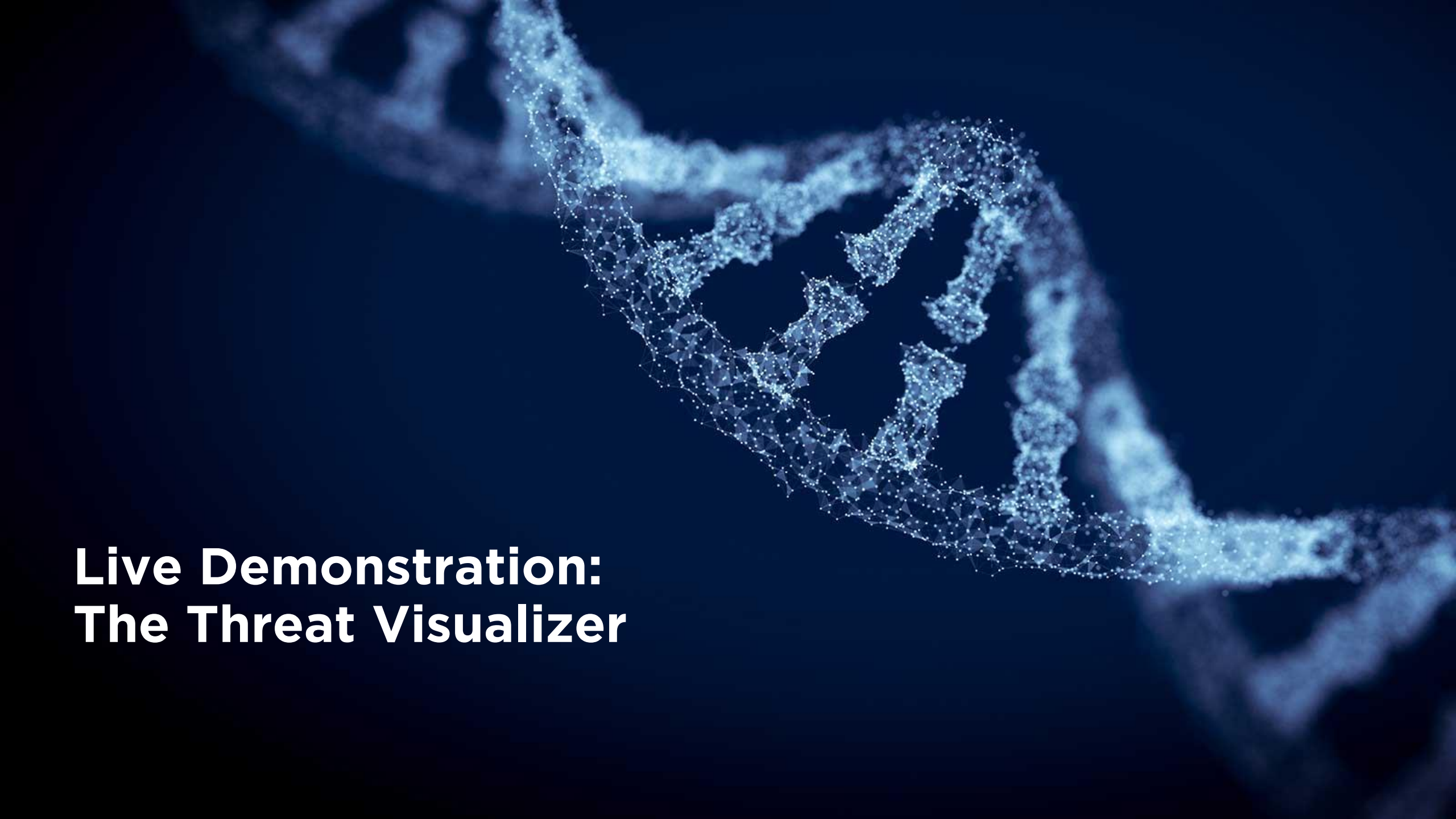
Industrial



Cloud & SaaS



Remote & IoT



# Live Demonstration: The Threat Visualizer

# Cloud Environment Compromised

**Industry:**
Financial Services

**Point of entry:**
Third-party cloud

**Apparent objective:**
Gain access through an exposed cloud environment to exfiltrate data

- Organization misconfigured cloud deployment, leaving critical server exposed to the Internet
- Server was continuously attacked by outside threat-actor attempting to gain access
- Darktrace identified the pattern of attack and alerted the customer to the ongoing risk

# Compromised Equipment on Assembly Line

**Industry:**
Food Manufacturing

**Point of entry:**
Connected manufacturing devices

**Apparent objective:**
Take control of Industrial IoT to infiltrate information

- Unknown attacker targeted devices on manufacturing assembly line to gain a foothold into the corporate network
- AI identified infected devices, even though security team was unaware they were connected to Internet
- Darktrace identified several issues with the firewall that were then remediated

# Conclusion

- Stealth and sophistication of threats are increasing
- Digital complexity creating new threat vectors and expanded attack surface
- AI cyber defense enables proactive approach
- Autonomous response is the future of cyber defense


Q&A