Artificial Intelligence-enabled cybersecurity is increasingly necessary

Cyber analysts cannot keep up with increasing cybersecurity threats

56% of the firms surveyed say their cybersecurity analysts are overwhelmed
23% indicate they are not able to successfully investigate all identified incidents
42% report an increase in incidents through time-sensitive applications

Organizations are increasing the pace of adoption of AI in cybersecurity

Nearly 1 in 3 organizations used AI in cybersecurity pre-2019
Almost 2 in 3 organizations plan to employ AI by 2020

How organizations are benefiting from AI in cybersecurity

- Share of organizations that have experienced cost benefits
- Decrease of 1-15%
- Decrease of more than 15%

- Share of organizations that have experienced time savings
- Decrease of 1-15%
- Decrease of more than 15%

- Detection
- Predictions
- Response

Where should organizations focus their AI cybersecurity initiatives?

- Anti-Exploit technology
- User Behavioural Analysis
- Behavioural Analysis to prevent Bot spam
- Scoring Risk in a network
- Endpoint protection
- Security orchestration, automation and response (SOAR)
- Data protection and compliance
- Malware detection
- Fraud detection
- Intrusion detection
- User/Machine Behavioural Analysis

Building a roadmap for implementing AI in cybersecurity

- Select high impact use cases
- Identify and create operational AI platforms
- Collaborate externally to enhance threat intelligence
- Training Cyber-analysts to be AI ready
- Select the right set of use cases to accelerate and maximize benefits
- Deploy SOAR to improve security management
- Install governance for AI in cybersecurity to deliver long-term improvement transparently and ethically

This message contains information that may be privileged or confidential and is the property of Capgemini. Copyright © 2019 Capgemini. All rights reserved.