DevSecBot

Andy Huang, Cyber Market Hub

andy@cybermarkethub.com

Humans are blessed with a brain that performs higher tasks from cognitive intelligence to mundane tasks.

Human Brain is best served to focus on problem-solving tasks and productive activities.

Automating Repetitive and Mundane tasks has always been the natural trend

To Automate ~~or Not~~

- Increase Architecture Complexity.
- More time and resources to focus on the appropriate processes.
- Consistency, Accuracy, Speed

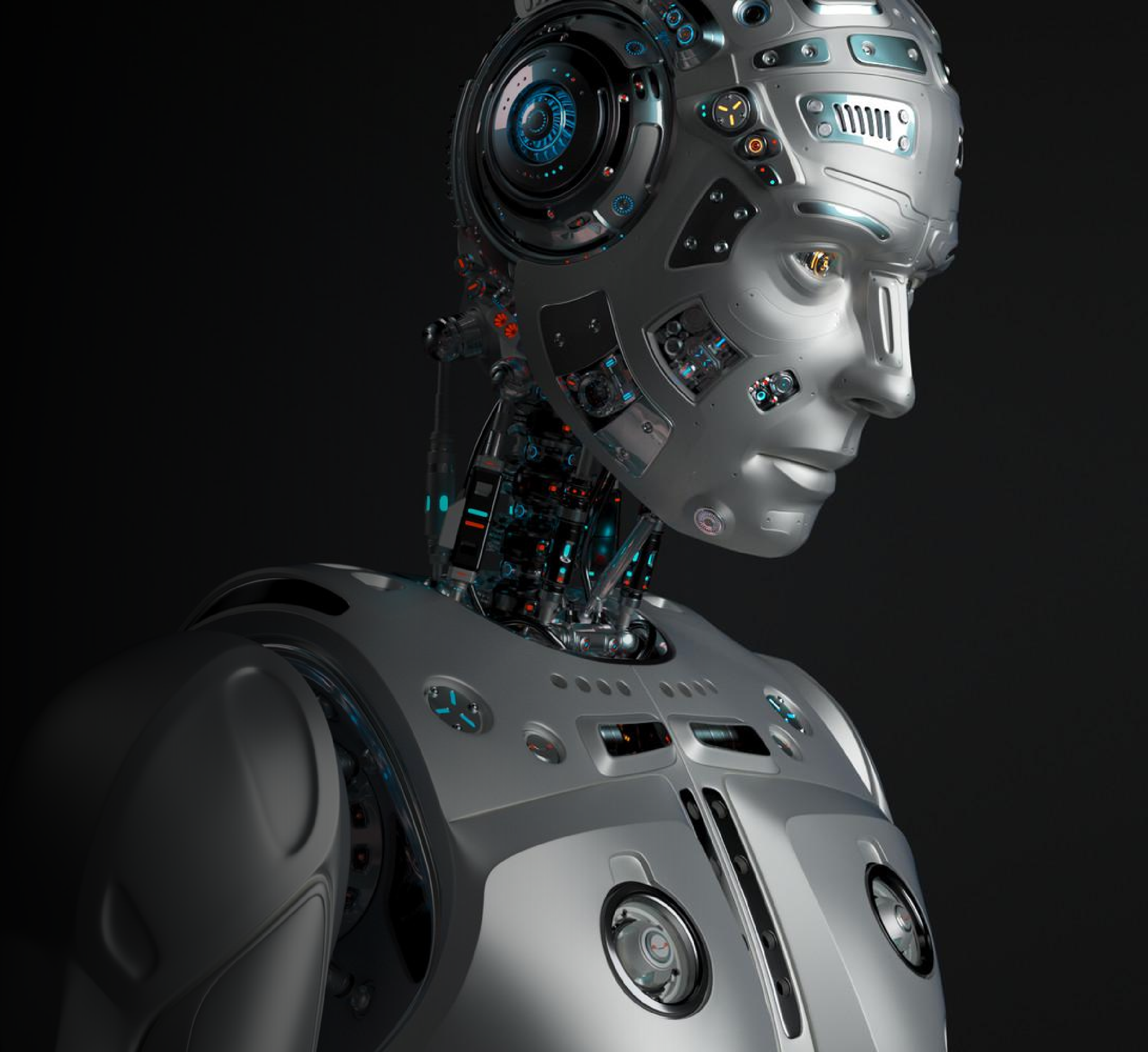
Automation Paradigms

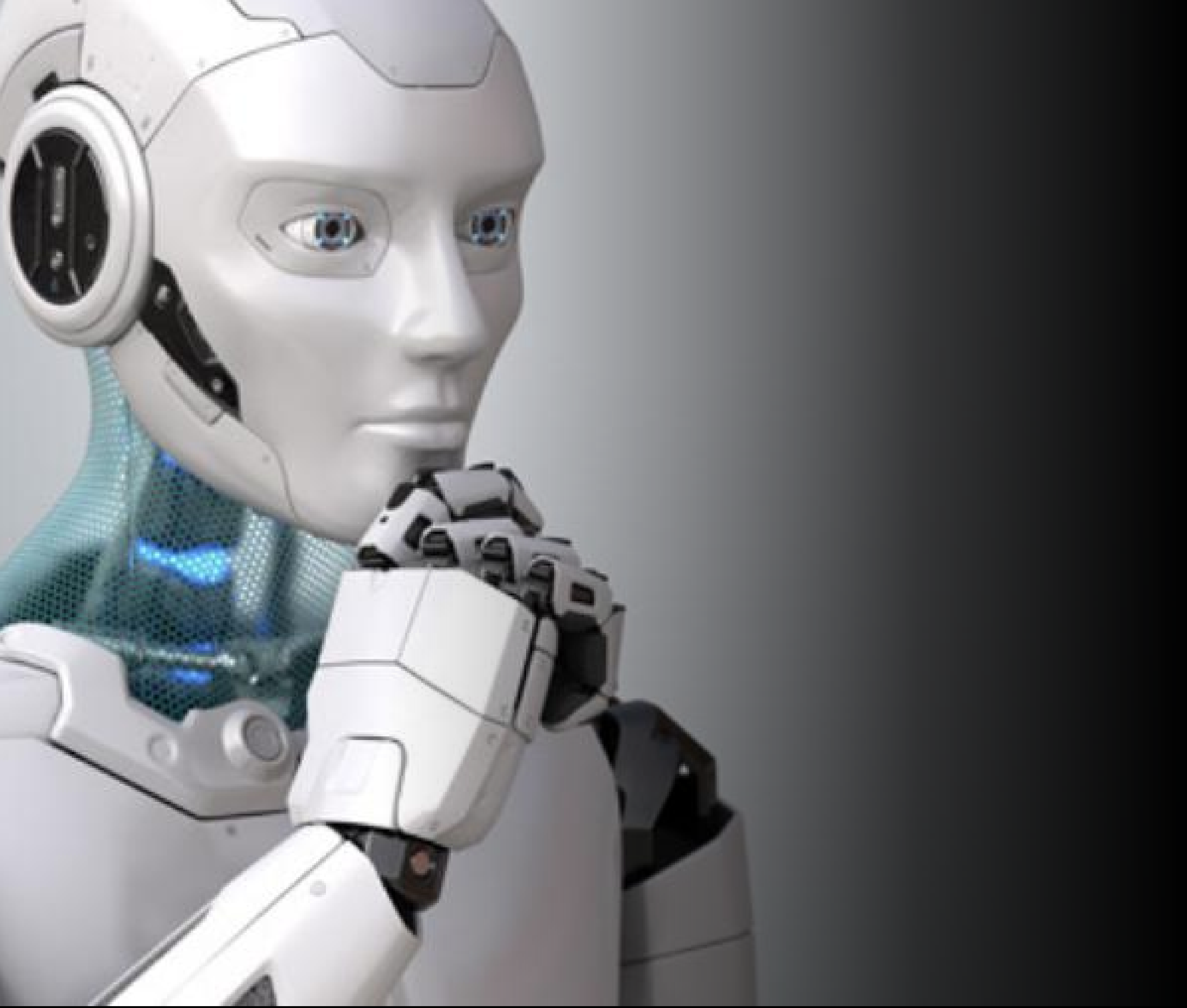
- Autonomous Test Tools
- Custom Developed Software and Codes
- Security Automation & Orchestration (SOAR)
- Robotic Process Automation (RPA) - BOTS

“Traditional” Implementations of BOTS

- To steal financial and personal information
- To attack legitimate web services
- To extort money from victims
- To make money from zombie and botnet systems

Time for the AutoBots





Why BOTS

- "cheaper, better, faster“
- "better, betterer, betterest“
- "futurise“
- "1/3 + 2/3 > 1"

Use Case #1
SOD Violation

- Audit Finding: Master Data Maintenance + Entry of/Changes to Sales Orders
- Mitigations
  - Master Data Tables made accessible only to Bot
  - Review Committee approves Changes to Pricing Table
  - Change Request sent to RPA Services Team.
  - RPA Services Team configures BOT to update System
  - Access Credentials assigned to BOT Services Team

Use Case #2: Access Certification

- Bots replaced manual validation checks of precertification data, campaign checks during access certifications and reviews, certification configuration management.
- As well as post certification reconciliation and reporting with automated processing diminishes unauthorized access and PII data looting.
- Outcome: An increase in the operational and cost efficiency gains by up to 45%.

Use Case #3: Security Hardening

- Bots have been programmed to perform Security Hardening of Servers
  - Run CIS Benchmark Scripts
  - Manually Configure Additional Parameters
  - Run Hardening Reports
- Outcome: Security Hardening Tasks are now performed whenever required.

Use Case #4: Firewall Configuration

- Bots have been programmed to manage Whitelisting and Blacklisting
  - Automatically update multiple Firewalls Blacklist with daily list of Malicious Domains and IP Addresses.
  - Automatically remove Domains and IP Addresses from Blacklist
- Outcome: Whitelisting Tasks are now performed whenever required.

Use Case #4: Inventory Tracking

- Operational Issue: Requires Tracking of Assets to Component level
- Mitigations
  - Bot programmed with different flavors of discovery tools
  - Implemented Rule-based Discovery
  - Continuous Monitoring of the inventory and update when Risks are uncovered.
  - Automate Risk Classification by applying cognitive learning to previously detected data.

Use Case #5: Security Operations

- Operational Issue: Slow investigation response on Suspicious Email
- Mitigation
  - Install Bot in VDI with Security Software
  - Bot downloads Suspicious Email
  - Bot disable Intranet
  - Bot runs Security Checks
  - Bot sends Status to SOC
- Improvements
  - 365x24x7 Investigation by Bot

“PREDICTION”

The CISO can be the next Iron Man of the Organisation

Discussion Points

- How do we see Bots being part of the IT
- Will Bots be part of an organisation’s cybersecurity strategy
- What are the foreseeable issues with Bots in Cybersecurity

Thank You