Inspiration from the unexpected

CYBER SECURITY TECH SUMMIT EUROPE

Martin Borrett
IBM Distinguished Engineer
CTO & Technical Executive – IBM Security Europe

March 13, 2019
PROGRESS

- Full privilege access
- Optional encryption
- Weak passwords
- Technical focus
- Compliance driven
- Least privilege access
- Default encryption
- Multi-factor authentication
- Boardroom focus
- Intelligence driven
Criminal Innovation is Thriving

- Shared revenue models
- Market-driven agile development
- Code and exploit reuse
- Lower barriers to entry
AI:
Attack tools get smarter

Cloud:
Attack surface gets bigger

IoT:
Attack targets get physical

Automation:
Attack campaigns get faster

Threat Actors:
Innovative
Opportunistic
Autonomous
Threat Responders

Innovative
Opportunistic
Autonomous

AI
Attack tools get smarter

Cloud
Attack surface gets bigger

Automation
Attack campaigns get faster

IoT
Attack targets get physical
FORCE MULTIPLIERS

Get Smarter

Respond Faster

Work Together
AUGMENTED INTELLIGENCE
1.24M
unstructured documents

10B
structured elements

24x
faster response times
GET SMARTER WITH AI

Scan source code  Discover personal data  Identify fraud  Find risky users  Predict threats
SECURITY ORCHESTRATION
Coordination is critical

- Verify alert from alerting source
- Lookup system details in active directory
- Match any artifacts with known bad...
- LDAP reset
- Carbon Black
- Executives involved
- CB IOC Hunt
- LDAP lookup
- CMDB Lookup
- Incident escalation
- Evaluate risk of disruptive response
- Evaluate risk of threat to enterprise
- Lookup system details from asset...
- Reset user credentials
- Search estate for relevant indicators
- Create and circulate status report
- Verify alert from source
- Verify if threat intelligence is known
- Evaluate risk of disruptive response
- Executive involved
- Incident escalation
- PEOPLE
- PROCESS
- TECHNOLOGY
Security Orchestration and Automation

- Verify alert from alerting source
  - Lookup system details in active directory
  - Match any artifacts with known bad...
  - Lookup system details from asset...

- LDAP lookup
- CB IOC Hunt
- CMDB Lookup

- Executives involved

- Escalation path
- Incident escalation

- Verify alert from source

- Evaluate risk of disruptive response
- Evaluate risk of threat to enterprise
- Verify if threat intelligence is known

- Search estate for relevant indicators
- Create and circulate status report
- Reset user credentials
- LDAP reset
- Carbon Black

PEOPLE            PROCESS            TECHNOLOGY
PRACTICE YOUR PLAYBOOKS
LESSONS LEARNED

Culture counts
Playbooks crack under pressure
Leadership matters
X-Force Command
Cyber Tactical Operations Center
STRONGER TOGETHER

Customers  Vendors  Researchers  Governments  Academics
WE ARE OPEN, JOIN US
IBM Security Connect
The platform to drive collaboration

Catalog
Applications | Solutions | Services
from Vendors, Partners, Clients, etc.

Cloud Platform
AppDev Framework | Data Integration | AI and analytics | Threat Intel

Existing infrastructure
On-premises security tools and infrastructure | Public and private clouds | Mobile devices and endpoints

IBM | ArcSight | splunk | McAfee | paloalto
AWS | Amazon | VMware | Cisco | Carbon Black
Ciscosentry | Cognizant | Deloitte | Qualys | Tenable

The platform to drive collaboration

IBM Security Connect
Visit us
IBM X-Force COMMAND CTOC

Sign-up
IBM X-Force Exchange
exchange.xforce.ibmcloud.com