Building an Effective Threat Intelligence Capability

Haider Pasha, CISSP, C|EH
Director, Security Strategy
Emerging Markets
Office of the CTO
Your Data casts a Digital Shadow that grows with every online interaction!
Already **Compromised**...

EXPANDED ATTACK SURFACE

• Cloud Infrastructures
• Mobile Protection
• Internet of Everything (IoT)
• BYOD

LARGE, COMPLEX ENVIRONMENTS

• Multiple Products
• Thousands of Servers
• Multiple Endpoints
• Lack of Talent

ADVANCED ADVERSARIES

• Well-funded
• Country Sponsored
• Nation States
• Underground Market

BROAD-BASED IMPACTS

• Targeted Attacks
• Internet of Everything
• More Data at Risk
• Disguised Attacks
A MAJOR SKILLS GAP IS EMERGING

“I HAVE LOTS OF DATA..... BUT NO INFORMATION”

“DATA SCIENCE” IS UNDER-INVESTED, NOT WELL DEFINED AND UNDER-SKILLED
Threat Intelligence Framework | A LIFE-CYCLE

- Data Classification
- Confirm and prioritize Risk
- Automated Response
- Incident Response
- Indicators of Compromise (IoC)

Build Critical Capabilities

Threat Intelligence Capability
Build Critical Capabilities | USING INDICATORS OF COMPROMISE

Suspect Indicator

“Big Data Enabled” Indicator Search

“Big Data Enabled” Attack Attribute Analysis

“Big Data Enabled” Campaign Analysis

“Big Data Enabled” Victim & Adversary Analysis

Build Protection Strategies

Deploy, Collaborate & Share

“Big Data Enabled” Intelligence Aggregation

Indicator of Compromise (IOC) or Breach

Actionable Security Intelligence & Cyber Protection

Copyright © 2016 Symantec Corporation
Cyber Security Exercise: Simulation-based Learning

Cyber Security Exercise strengthens cyber-readiness through live-fire simulation of today’s most sophisticated and advanced targeted attacks

**THINK LIKE AN ATTACKER**

- Cloud-based, virtual training experience simulates multi-staged attack scenarios allowing users to take on the identity of their adversaries
- Gamification provides a more engaging, immersive educational experience
- Frequent content updates ensure scenarios are current on latest adversaries, motives and techniques
- Scenarios contain research from Symantec security experts, threat analysis and current threat landscape

**BENCHMARK AND ADVANCE YOUR SECURITY TEAM**

- In-depth security skills reporting
- Structured recommendations for cyber security skills development
- Identify skills gaps in your security team and build training plans accordingly
- Prescreen and recruit new security experts internally and externally
Cyber Security Exercise
Continuous skills development for Security Teams

- Fully managed SaaS and Platform-as-a-Service offering with global coverage
- Comprehensive scoring and reporting functionality
- Over 600 hours of live system challenge scenarios, covering different industry verticals
- Over 7,000+ participants in 30+ countries
- Scenarios designed for different levels of difficulty
- Exercises can be run 1 day monthly, quarterly or yearly
Threat Intelligence Framework | A LIFE-CYCLE

Establish Sources

- Internal Sources
- Commercial & OSINT Sources
- Government Sources
- Industry Sources

Build Critical Capabilities

- Data Classification
- Confirm and prioritize Risk
- Incident Response
- Automated Response
- Indicators of Compromise (IoC)
- Analyst Diversity
- Career Advancement
- Development Program
- Cyber Simulations

Develop Analyst Skills
Establish Sources | **RICH TELEMETRY**

**Internal Sources**
- Crowdsourcing
- Employee Security Awareness
- Internal Forums / Distribution Lists
- Log and network data (SIEM, FW, etc.)

**Industry Sources**
- Supply Chain Partners
- Informal Industry Relationships (1-on-1)
- Formal Industry Organizations (ENISA, etc.)

**Open & Commercial Sources**
- Vendor Threat feeds
- Security Intelligence Providers
- Public Threat Feeds (Zeus, SpyEye, etc.)
- Counter Intelligence & HUMINT capability
- Software-as-a-service (SaaS) threat alerting

**Government Sources**
- Law Enforcement
- National Security Organizations
- Computer Emergency Readiness Teams (CERT)
Threat Intelligence Framework | A LIFE-CYCLE

Operationalize Intelligence
- Proactive Defense
- Threat Dissemination
- Threat Analytics
- Internal Sources
- Commercial Sources
- Government Sources
- OSINT & HUMINT Sources

Cyber Kill Chain

Data Classification
- Confirm and prioritize Risk
- Incident Response
- Analyst Diversity
- Career Advancement

Automated Response

Indicators of Compromise (IoC)

Development Program

Cyber Simulations

Establish Sources

Build Critical Capabilities

Develop Analyst Skills
“The ability to gather & query both external insight and internal visibility, essentially generating security intelligence, needs to be at the heart of any (big data) security analytics platforms”

Providing better protection by:

✧ Predictive Analysis & Adversary Intelligence
✧ Earlier Event Detection & Prioritization
✧ Faster Incident Response & Better Risk Management
Symantec is the leader in cyber security big data analytics for many years……

1 billion+ systems

200M+ Norton & SEP users (the biggest source of telemetry)

4 trillion rows of security telemetry
100 billion more/month

9 security ops centers globally;
1000+ expert analysts

Blocked 182 million threats
last year

Copyright © 2016 Symantec Corporation
Symantec Enterprise Security Strategy
Integrated Solutions, Now with Bluecoat

Common Platform and Cloud Services
(Integration, Analytics, Orchestration, Provisioning, Usage, Metering, Licensing, Identity Management)

Common Cloud Infrastructure (IaaS): Public or Private Cloud

SaaS/IaaS

PUBLIC CLOUD

PRIVATE CLOUD

On-Premise DATA CENTER

Common Cloud Console – Management

Threat Protection
ATP
Endpoint
Web Proxy
DC Security
Email Security

Information Protection
DLP
CASP
VIP 2FA
Managed PKI
Encryption (SSL)

Analytics & SOC
Unified Analytics
Platform and Apps
Cyber Security
Services (CSS)

Management & Compliance
EPM
Control Compliance
Suite (CCS)

Common Platform and Cloud Services

SELF SERVICE
PARTNER RE-SELL
DIRECT SELL
Thank you!

haider_pasha@Symantec.com