Emtec

Business & Technology Empowered

Digital Cyber Security meets Digital Service Management

Cyber Risk Management In a Digital World

September, 2019

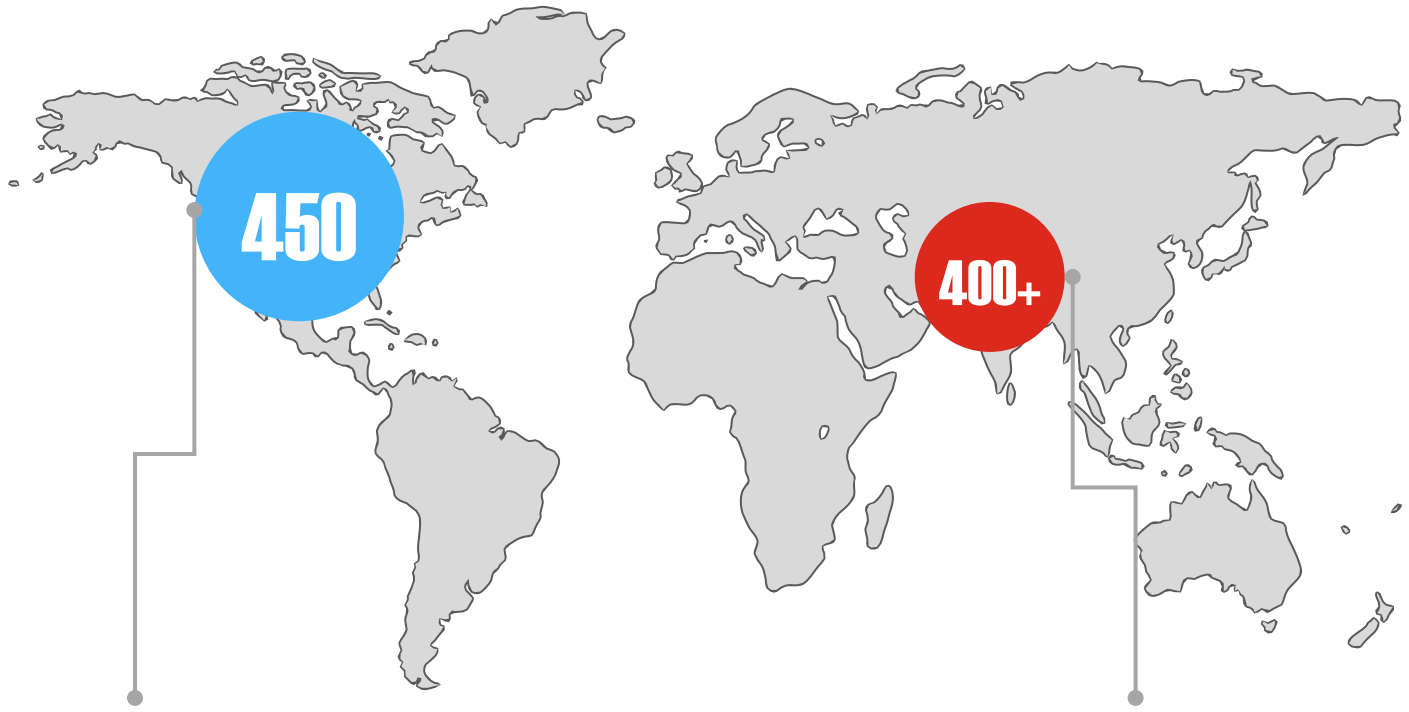
Agenda

- Introduction to Emtec
- Features of the Digital World
- Cyber Security in a Digital World
- Digital ITSM driving Digital Security

Emtec
CONFIDENTIAL | © 2016 Emtec, Inc.

About Emtec

Onsite / US-Remote - Offshore - Nearshore - Blended



NORTH AMERICA OFFICES

USA (9)
CANADA(2)

INDIA OFFICES

Pune
Bangalore

22+ YEARS IN BUSINESS

1,000+ CLIENTS

850+ CONSULTANTS

250+ CLOUD PROJECTS

200+ APP DEV CLIENTS

2,500+ PROJECTS

Practice Summaries

Technology empowered business solutions through 3 practices

Emtec Consulting Services (ECS)

- *On Premise*
- *Cloud*
- *Managed Services*

Backend Integration & Maintenance

Emtec Digital Services (EDS)

- *Custom Applications*
- *Mobility Solutions*
- *SalesForce.com Development*
- *Managed Services*

User Experience Design, Development, & Automation

Emtec Infrastructure Services (EIS & EPS)

- *Infrastructure Managed Services*
- *ITSM/ESM*
- *Security & Compliance*
- *Managed Services*

Infrastructure Management

End-to-End Solutions For Enterprise Digital Transformation

Consulting

Strategy, governance, process

Applications

ERP, HCM, CRM, app, development, mobile solutions

Cloud

Applications, Infrastructure, Blockchain

Analytics

Enterprise reporting, Predictive analytics, big data

Intelligent Process Automation

AI/ML, IOT, Cognitive, RPA, Test Automation

Client Snapshot

We are dedicated to driving true value for our clients in everything we do.

Compliance & Security Services



Advisory Services

- Data Protection Impact Assessment (DPIA) Process
- Article 30 Record of Processing Activities
  - Data Source Identification
  - Data Mapping
- Privacy 3rd Party Contracts Review

Governance

- Privacy Policy Development/Remediation
- Data Subject Access Request (DSAR) Process Development and Implementation
- Data Minimization

Tools & Operations

- Tools Implementation
- Managed SIEM & SOC
- AI based threat detection

Development & Support

- Data Protection Office (DPO) Support
  - Collect information to identify processing activities
  - Analyze and check processing activities for full compliance with the GDPR
- Ongoing Compliance and Privacy Training Program
- Incident / Breach Response and Investigation

Characteristics of the Digital World

Every rich feature of the digital world represents an Risk Management challenge

The Scale of Technology in a Digital World

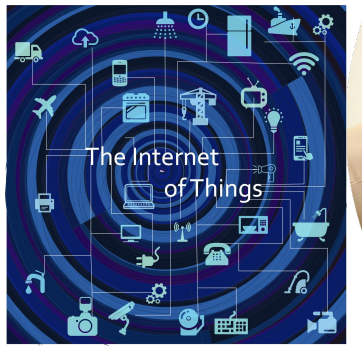
- Exponential growth
- Nanotechnology
- Geographic scale

The Pace of Technology in a Digital World

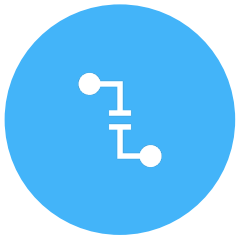
- Exponential growth
- Danger at the speed of light
- Limitless connectivity

The Scope of Technology in a Digital World

- Consumerization
- Deep and Wide Expertise
- Arms Length Deployment
- Pervasive Access



Digital World Challenges for Service Management



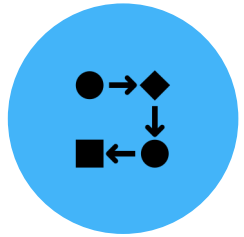
ITSM SUPPLANTED BY ESM

ITSM PROCESS REQUIREMENTS BEGIN EARLIER, GO DEEPER

SCALE SHOULD NOT COMPROMISE CAPABILITY

TOOLS AND PLATFORMS MUST BE PART OF THE DIGITAL WORLD

VISIBILITY IS CRITICAL



INTELLIGENT AUTOMATION IS KEY

Digital World Implications for Security

- Traditional boundaries no longer exist
- Swivel seat approaches cannot work at scale
- What is my threat surface?
- Exploitation is a digitally enabled business
- Time from vulnerability initiation to exploitation will continue to shrink
- The cost of an exploitation in a Digital World is staggering
- Digital World problems require Digital Solutions

Cyber Security in the Digital World

Effective Cyber Security Leverages Digital Capabilities inherent in ITSM

Digital Security – Digital ITSM Symbiosis

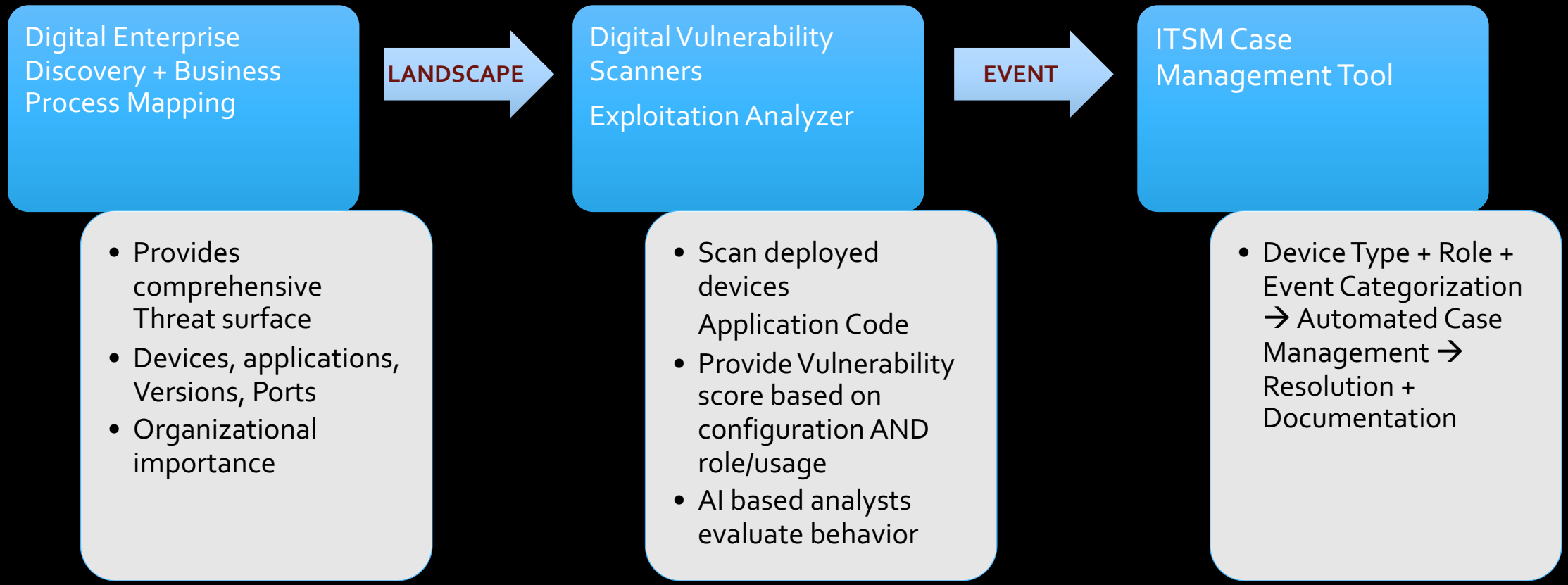
Digital ITSM

- Discovery and event notification at scale
- Business process ←→Resource (Human and technology) mapping
- Accurate, Current CMDB
- Sophisticated yet agile process workflows
- Service orchestration at scale
- Business process sensitive case management
- Resolution automation
- Service execution validation
- RPA and Service integrations
- Smart Reporting - Compliance

Digital Security

- 3 Dimensional approach to security
  - Environmental Awareness – What do I have to protect?
  - Vulnerability Intelligence – What are known threats and how am I exposed today?
  - Risk Consciousness - How am I being exploited currently?
- Contextual evaluation of all dimensions
  - What is the impact of an exploit ?
  - Which exploits potentially disrupt my business most?
- Context aware case management
  - Risk minimization vs cost management
  - Remediation at scale

How do these Capabilities Complement each other?



Digital Security Building Blocks – Threat Surface Management

- **Enterprise Discovery** to address:
  - Awareness of constantly evolving technology environment
    - End user devices, IOT, role specific Cloud services, SaaS providers
    - Internal and 3rd party datacenter platforms
    - Infrastructure cloud
  - Platform Relevance to business services
  - Currency control – frequency of scans based on sensitivity of platforms

- **Digital Security Services Output**
  - Threat Surface with business relevance
    - Current map of all business services and every component delivering these services
    - Consumed by Vulnerability Analysis + Active Treat Detection
  - Updated CMDB → drives case management

Digital Security Building Blocks – Vulnerability Assessment

- **Digital Vulnerability Analysis** to address:
  - Awareness of constantly evolving attack vectors
    - Recognizing configuration vulnerabilities
    - Realtime threat intelligence
  - Digital platforms with Machine learning for fundamental assessment
    - Experienced analysts to tune tools and handle marginal cases
  - Leverages Business Role information to establish business vulnerability score
  - Digital Analysis of custom code to identify inherent vulnerabilities in approach or libraries
  - Executed on a daily/weekly/monthly basis for various business environments

- **Digital Security Services Output**
  - Use attack vectors + platform role to provide vulnerability score
  - Macro view - Vulnerability scores drive call to action at executive level
  - Micro Level – Identified vulnerabilities provide case management triggers
    - Incidents initiated in SM tool → categorization, automated actions, notifications, visibility
    - Vulnerability passed to security analytics platform → AI based scans to determine if the vulnerability has been exploited

Digital Security Building Blocks – Active & Unknown Threat Discovery

- **Digital Security Advanced Analytics** to address:
  - AI platform that learns the environment and identifies threats based on:
    - Recognizing behavioral changes
    - Known vulnerabilities and threats
    - Organizational business model characteristics
    - Rules and signatures as a complementary source of threat intelligence
  - Multimodal Machine learning for fundamental assessment
  - AI analysts to provide context based evaluation of log data and 3rd party date from other SIEMS
  - Comprehensive log analysis

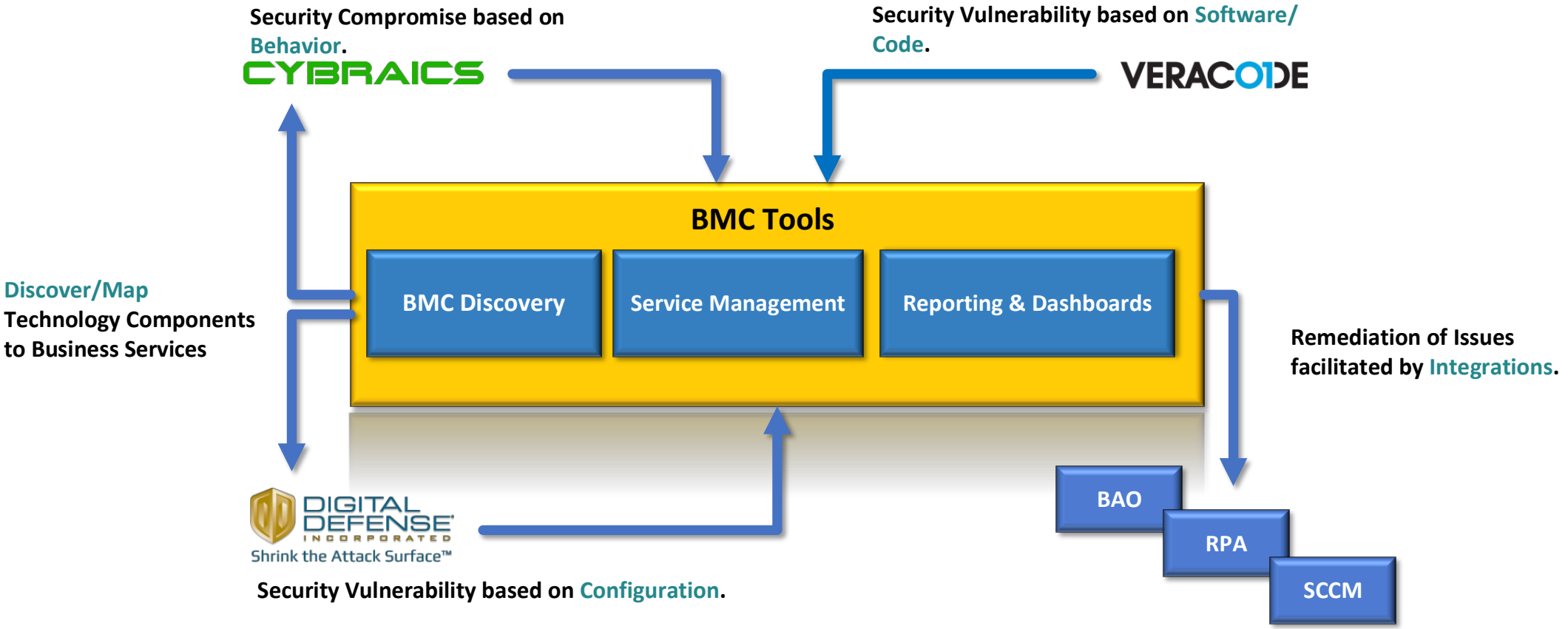
- **Digital Security Services Output**
  - Threat health score based on identified anomalies and role of anomalous devices/users
  - Macro view - Vulnerability scores drive call to action at executive level
  - Micro Level – Identified vulnerabilities provide case management triggers
    - Incidents initiated in SM tool → categorization, automated actions, notifications, visibility, resolution

Digital Security Building Blocks – Case Management

- **Digital Security Case Management** to address:
  - Capturing Security Events for:
    - Recording, classification and historical analysis
    - Event management based on categorization of device and event
    - Problem and change management integration
    - Resolution process management
    - Compliance process management
  - Facilitates orchestration for resolution consistency at scale
  - Drives resolution automation – including RPA and other automations

- **Digital Security Services Output**
  - Managed event processing with integrated workflows and reports
  - Dashboard view of exceptions and standard case progress
  - Automated compliance process reporting and notifications
    - Domain specific compliance processes
    - Impact based reporting and notification
  - ITSM analytics applied to security management

Sample Digital Security Platform Footprint



- BMC Discovery to map a complete picture of the Infrastructure.
- Service Management for Security Requests.
- Smart IT for the remediation of Security Events.
- Smart Reporting for reporting and dashboards.

Takeaways

- Digital Service Management is the start and finish of the digital Security Model
- Core ITSM components are essential – Discovery, CMDB, Workflow, Orchestration, Automation, Smart Reporting
- Vulnerability analysis should be neither static nor infrequent – leverage digital
- Code analysis can be injected into the code development process -
- Keep Them Out – Focus on Prevention + resolving vulnerabilities
- Seek Them Out – Evaluate whether vulnerabilities have been (are being) exploited
- Automate resolution
- Use digital services to address scale – AI, ML, RPA

Questions ??

https://www.emtecinc.com/services/infrastructure/managed-cyber-security-services/