RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

Connect to Protect

SESSION ID: SOP-T07

Next Generation Cyber Security Operations Centers

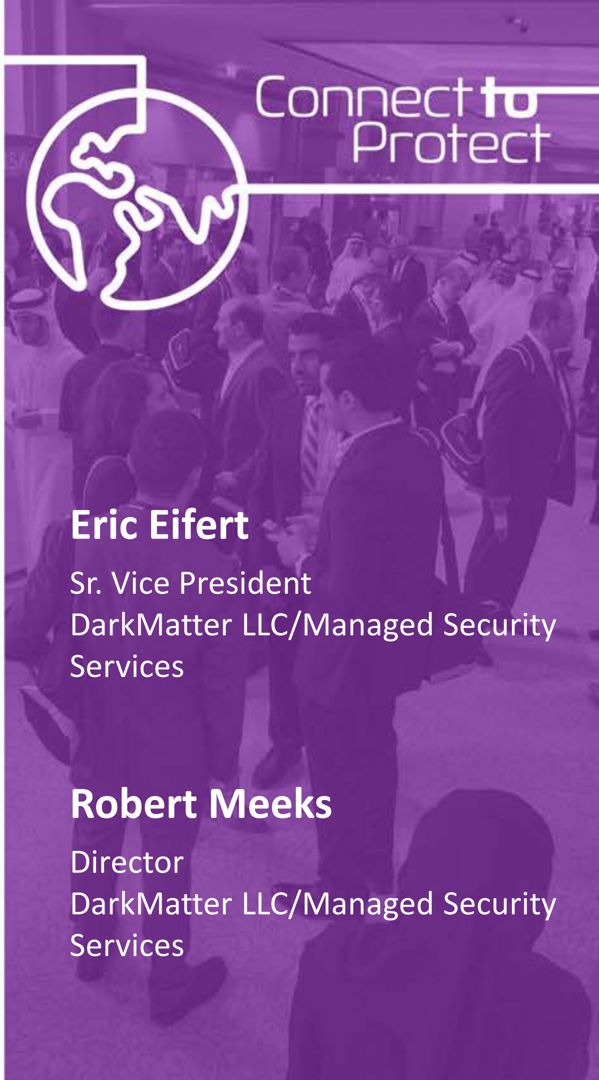
Eric Eifert

Sr. Vice President
DarkMatter LLC/Managed Security Services

Robert Meeks

Director
DarkMatter LLC/Managed Security Services

#RSAC



Eric Eifert Background

- Over 20+ years experience in Cyber Security
  - Special Agent investigating cyber crime, computer intrusions, cyber espionage, and cyber counterintelligence
  - Program Manager for large U.S. Cyber Security Operations Centers
  - Executive running cyber security line of business ($125+M)
  - Adjunct professor teaching graduate cyber investigations
  - SVP DarkMatter's Managed Security Services

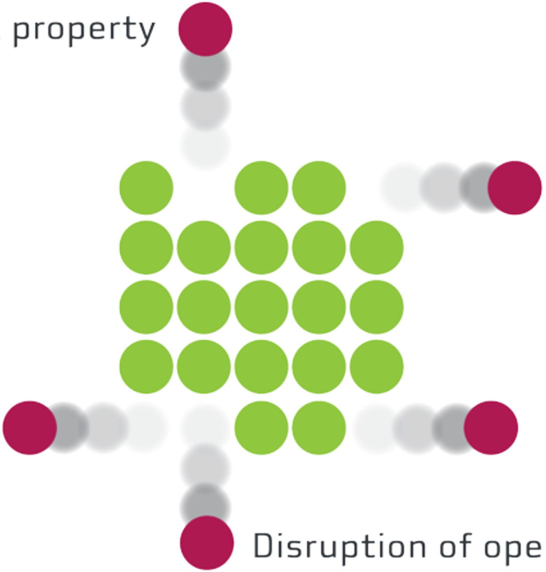
Robert Meeks Background

- Over 20+ years experience in Cyber Security
  - Base Network Security Officer CAFB
  - Operations Manager supporting MSS customers both Commercial and Federal. Also responsible for Cloud based Services.
  - MSSP Director for DarkMatter

Who are the Threat Actors

- World Trade / Globalisation Activists
- Environmental Groups
- Untrained Personnel
- Information Hacktivisists
- Corporate Intelligence
- Trusted 3rd Parties
- Insider Threats
- Illegal Information Brokers
- Regional Political Activism
- Investigation Companies
- Freelance Agents
- General Attacker Threats
- Non-State Sponsored Terrorism
- Competitors, Contractors, Corporations
- Nation States / Governments

What Are The Risks



Theft of intellectual property

Competitive disadvantage

Extortion + Cyber Ransom

Loss of reputation and corporate brand

Disruption of operations

Challenges

- Customers
  - Customer IT/Security Operations teams may not fully understand their Business, Assets and Threats
  - Need to optimize capital expenditures and reduce operation cost
  - Ability to maintain and fully utilize asset information
  - Lack of actionable and meaningful reporting and threat intelligence
  - Lack of human resources to meet all the security requirements
- MSSP’s
  - Limit themselves based on the legacy or internally developed SIEM tools
  - Utilizing unvalidated threat intelligence as content
  - Try to fit an alert into a preconceived conclusion
  - Fail to understand their customers Business, Assets and Threats (Enemies)
  - Focus on metrics that show the customer they are adhering to SLA’s
  - Fail at understanding sophisticated campaigns that span months or years

Know Thy Customer

- Strengths
  - Security Perimeters
  - Policy Enforcement
  - Auditing and Compliance
- Weaknesses / Challenges
  - Lack of awareness and tracking of assets
  - Struggle to keep up with outdated hardware/software and vulnerabilities
  - Budget constraints
  - Must adhere to specific boundaries and rules
  - Audit and Compliance is done as a snapshot in time

Know Thy Enemy

- Strengths
  - Underground community support
  - Anonymity
  - No boundaries, limitations or rules
- Weaknesses Challenges
  - Potentially funding (not the case with Nation States)
  - Lack of organization and structure
  - Originality and human error
  - Bragging and or claiming responsibility/credit

How to “Know Thy Customer”

- Understand their business and operational environment
  - What is it you are protecting (Reputation, Intellectual Property, Money, Operations, PII, etc.)
  - What security components do they have or are they missing
  - Understand their assets (Systems, Applications and People)
  - Identify Key assets (DB’s, Storage, VIPs etc.)
  - What are their regulatory and governance models
  - Understand their risk exposure and vulnerabilities
  - Understand their IT/Security strategy and roadmap

How to “Know Thy Enemy”

- Proper Threat Intelligence Program
  - Research who the threat actors are that are targeting you
  - What attack methods do they use
  - Focus on Indicators that provide a higher value of reward
    - TTP
    - Tools
    - Network/Host Artifacts
- Collect, store, and add value to the your threat intelligence
  - Use Intel IOC’s as context and not content (Unless verified a
  - nd even then its value is time sensitive)
  - Collaborate with Government agencies (CERTS)
  - Collaborate with Industry Peers

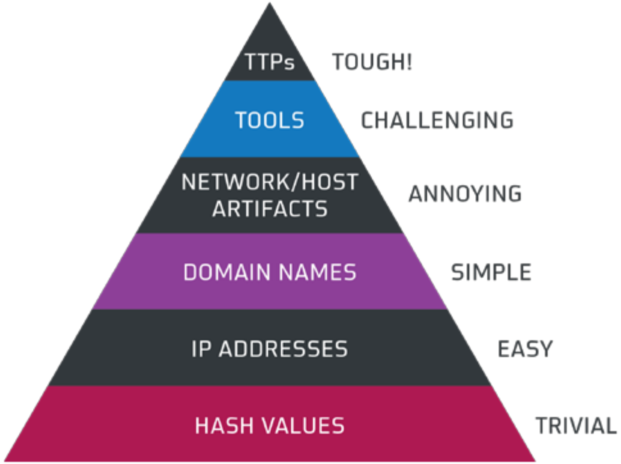
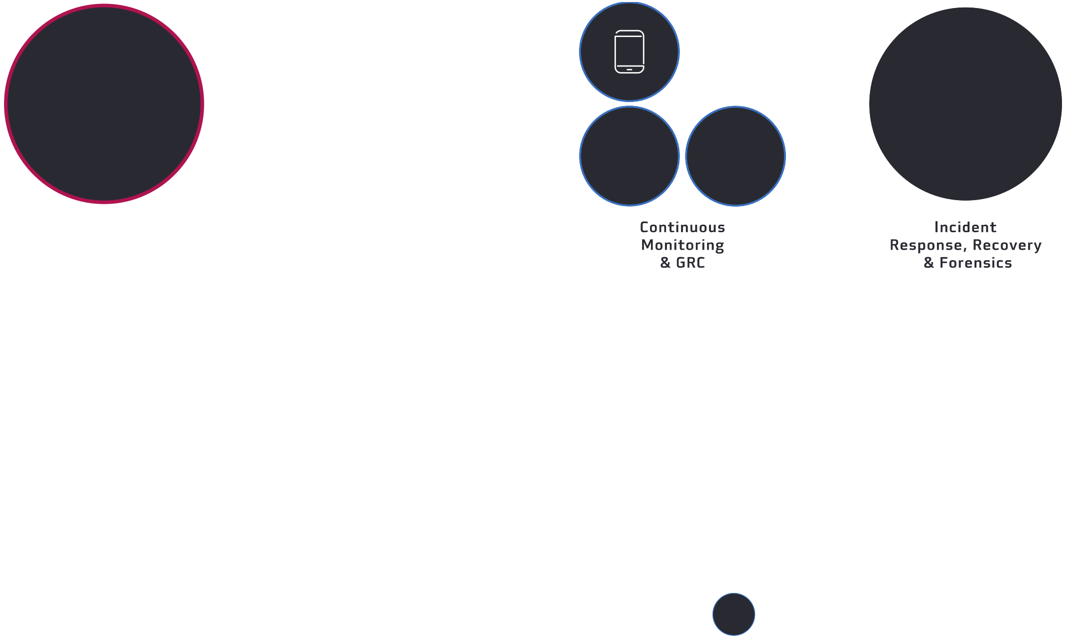


Image Sources: David Bianco’s the pyramid of pain

Next Gen Cyber Security Operations Centers


Continuous Monitoring & GRC
Incident Response, Recovery & Forensics

. THREATS

. ASSETS

. VULNERABILITIES

. RISKS

. COMPLIANCE

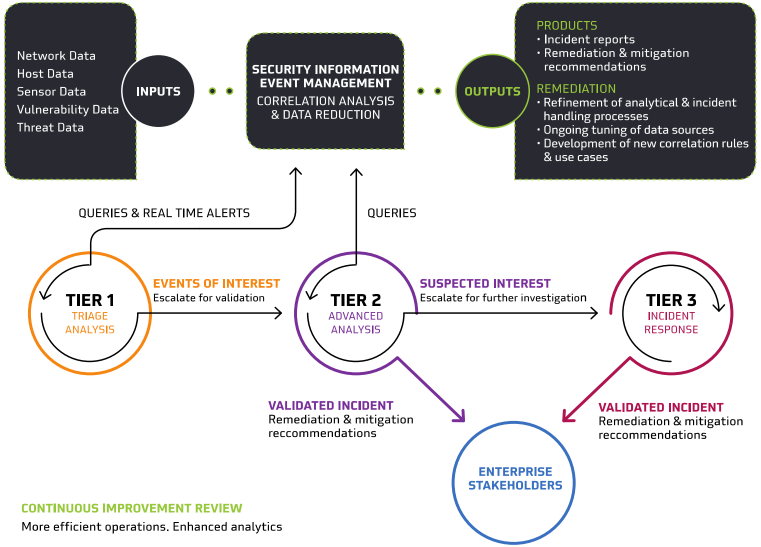
. INCIDENTS

Continuous Monitoring

- Continuous Monitoring provides continuous cyber situational awareness and not a snap shot in time
- Monitor your Risk and Governance adherence on an on-going basis
- Identify when changes in hardware, software, and users takes place
- Holistic view necessary to see across the entire business operations
  - Information Technology
  - Operational Technology (Industrial Control Systems/SCADA)
  - Internet of Things/Everything

Advanced Analytics

- Use every possible correlation methodologies
  - Behavioral
  - Statistical
  - Heuristical
  - Anomaly
  - Reputational
- Deploy Technology to provide visibility across all assets
  - Remote locations
  - Non-IP based
  - Mobile and wireless
  - Endpoints
- Integrate continuous monitoring and rapid (automated) remediation/mitigation activities



Network Data
Host Data
Sensor Data
Vulnerability Data
Threat Data

INPUTS

SECURITY INFORMATION EVENT MANAGEMENT
CORRELATION ANALYSIS & DATA REDUCTION

OUTPUTS

PRODUCTS
- Incident reports
- Remediation & mitigation recommendations

REMEDIATION
- Refinement of analytical & incident handling processes
- Ongoing tuning of data sources
- Development of new correlation rules & use cases

QUERIES & REAL TIME ALERTS

QUERIES

TIER 1
TRIAGE ANALYSIS

EVENTS OF INTEREST
Escalate for validation

TIER 2
ADVANCED ANALYSIS

SUSPECTED INTEREST
Escalate for further investigation

TIER 3
INCIDENT RESPONSE

VALIDATED INCIDENT
Remediation & mitigation reccommendations

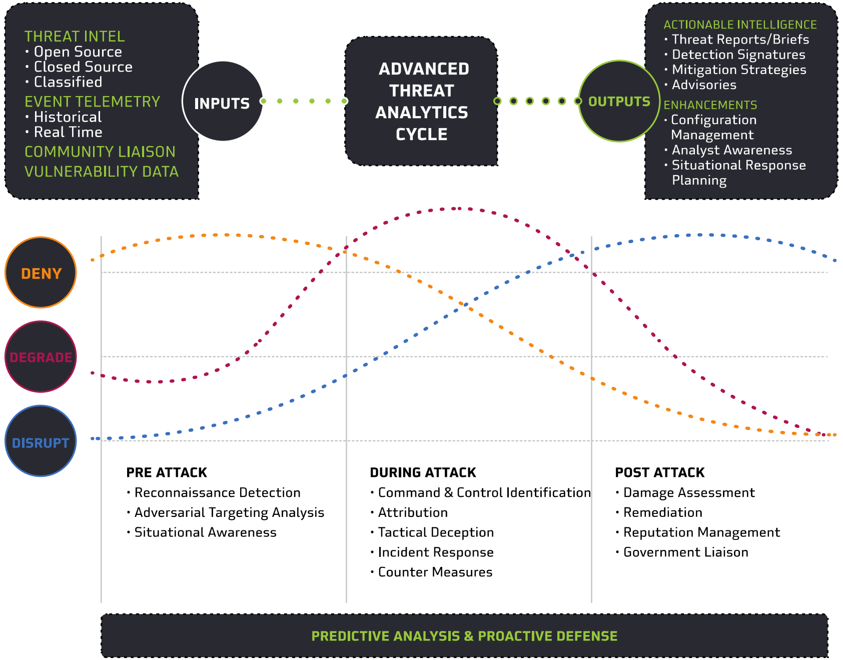
VALIDATED INCIDENT
Remediation & mitigation reccommendations

ENTERPRISE STAKEHOLDERS

CONTINUOUS IMPROVEMENT REVIEW
More efficient operations. Enhanced analytics

Advanced Threat Analytics

- Develop a threat intelligence program that truly adds value and context
- Enhance by doing validation on all intelligence feeds
- Develop partnerships with government information sharing programs
- Develop partnerships with industry peers to share threat intelligence
- Interface with all stakeholders to understand critical components



THREAT INTEL
- Open Source
- Closed Source
- Classified

EVENT TELEMETRY
- Historical
- Real Time

COMMUNITY LIAISON

VULNERABILITY DATA

INPUTS

ADVANCED THREAT ANALYTICS CYCLE

OUTPUTS

ACTIONABLE INTELLIGENCE
- Threat Reports/Briefs
- Detection Signatures
- Mitigation Strategies
- Advisories

ENHANCEMENTS
- Configuration Management
- Analyst Awareness
- Situational Response Planning

DENY

DEGRADE

DISRUPT

PRE ATTACK
- Reconnaissance Detection
- Adversarial Targeting Analysis
- Situational Awareness

DURING ATTACK
- Command & Control Identification
- Attribution
- Tactical Deception
- Incident Response
- Counter Measures

POST ATTACK
- Damage Assessment
- Remediation
- Reputation Management
- Government Liaison

PREDICTIVE ANALYSIS & PROACTIVE DEFENSE

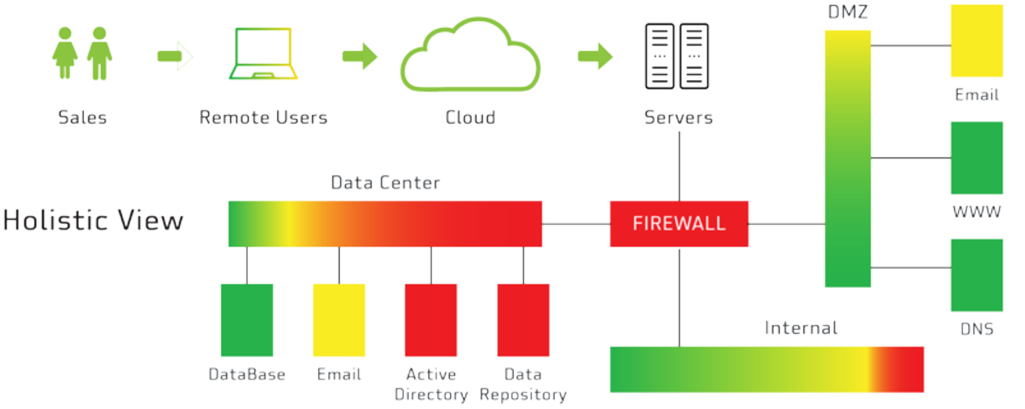
Problem of MSS Reporting

- # of Alerts per month
  - Does this really mean anything and it’s a snapshot in time?
  - Linking alerts across larger periods of time against assets and kill chain show value!
- Types of Alerts
  - What does this have to do with anything?
  - What matters is we let you know when your assets are being targeted and how the alerts have a relationship!
- Mean time to detect
  - Does it matter if I detect someone has stolen your data in 15min or 1 hour?….It’s gone!
  - What matters is that we let you know your server is at risk and we are seeing an attempt at data exfiltration!

Meaningful and Actionable Reporting

- Holistic approach of reporting
- Change management reporting based on validated risk exposure
- Analytical reporting based on identifying actual risks and incidents and not by hitting SLA
- Demonstrate value added service being provided

Holistic Dashboard View's Showing Value



User Type	Asset Priority
Exec. Managers	Critical
Domain Admins	Critical
Finance	High
HR	High
IT/DEV	High
Sales	Medium
Marketing	Low
Basic User	Low

Users

App Type	Asset Priority
Active Directory	Critical
Databases	Critical
WWW	High
Email	High
DNS	High
Data Repository	High

Apps

Holistic Score

System

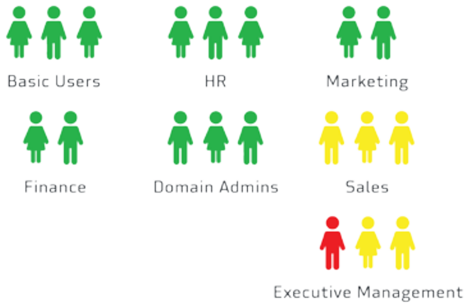
SystemType	Asset Priority
Security Stack	Critical
Network	Critical
Unix Servers	High
Windows Servers	High
Mac Endpoint	Low
Windows Endpoint	Low
Mobile Endpoint	Low

Threats

Threats	Risk Factor
Campaigns	Critical
Vulnerabilities	Critical
IOC's	Medium

Showing Value

Kill Chain Phase	App	System	Users	Threats
Recon	●			
Weapon				
Delivery		●		
Exploitation				
Installation				
C2C			●	
Action on Objective	●			



Conclusion

- The cyber domain has become the new battlefield and no one is immune to the effects of the battles that take place on a daily basis
- The threat landscape is getting more complex and hyper-connected
- The Future of MSS has to:
  - Have a holistic view of the battlefield
  - Know the strengths and weaknesses of their customers and their enemies
  - Understand customers business operations and how the cyber domain impacts their business
  - Understand the tactics of cyber attacks to understand how to protect their customers environment and critical assets

Questions?