Building Adaptive Security Operations

SOC v5.0

Tamer El Refaey
Chief Cyber Security Strategist, Emerging Markets
Micro Focus

24.10.2018

KEY SECURITY OBJECTIVES

REACH FURTHER

WORK SMARTER

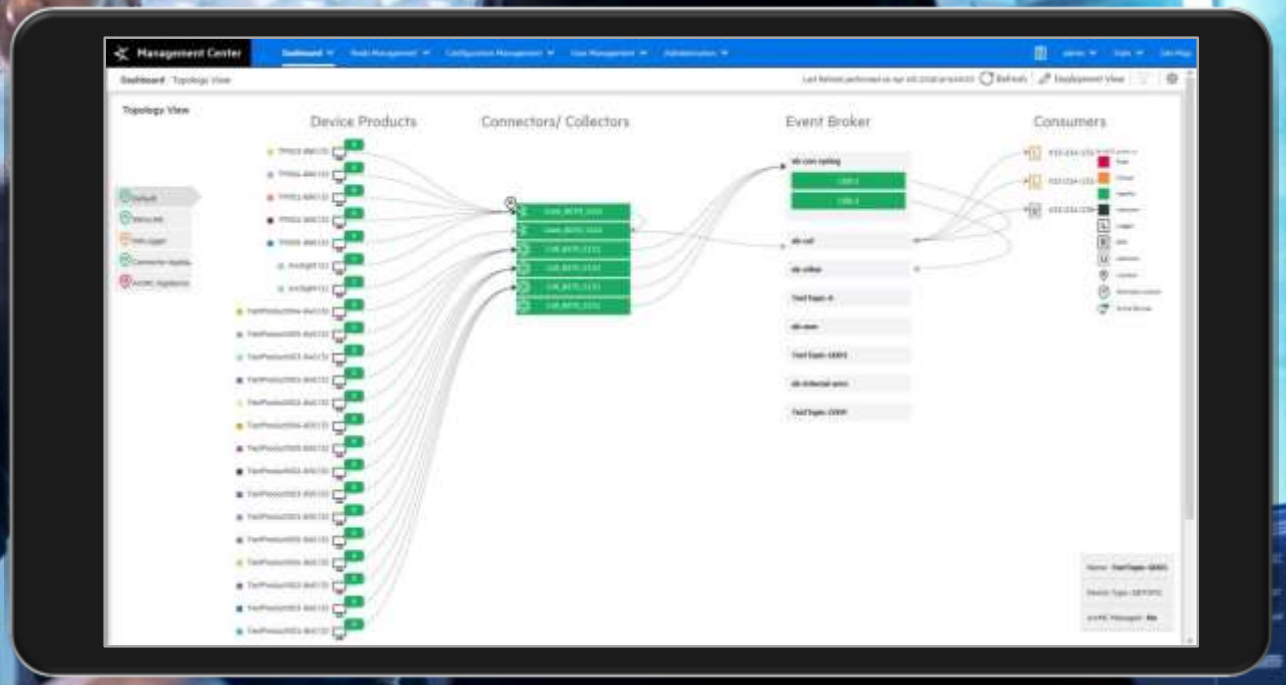
AVOID DISRUPTIONS

ACT FASTER


SECURITY OBJECTIVES
Act Faster
Avoid Disruptions
Work Smarter
Reach Further
Ensure Compliance
Compliance Based Log Management
ADAPTIVE SECURITY OPERATIONS JOURNEY
• "I'll keep everything"
• Audit
• Compliance reports
SOC CAPABILITY
Log collection
Real-time correlation & detection analytics
Machine learning and behavior analytics
Proactive hunting
Security Orchestration, automation and response

Compliance Based Log Management

- Data ingestion capabilities
- Log source monitoring
- Event normalization, filtering, categorization and enrichment
- Fast searches and reporting

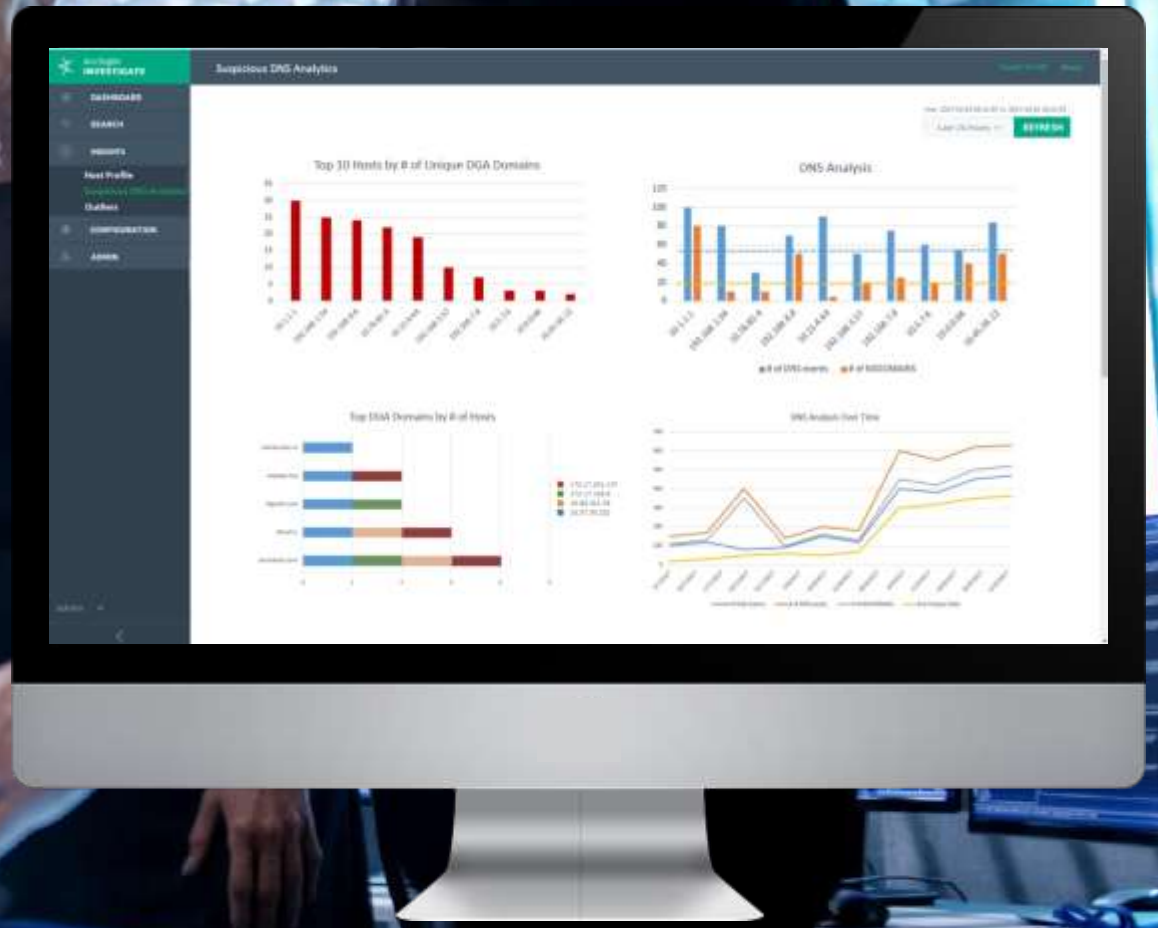


MICRO FOCUS


SECURITY OBJECTIVES
Act Faster
Avoid Disruptions
Work Smarter
Reach Further
Ensure Compliance
Real-time Correlation & Detection Analytics
• "What's happening now"
• Set monitors
• Use cases library
• Real-time Workflow
• "I'll keep everything"
• Audit
• Compliance reports
ADAPTIVE SECURITY OPERATIONS JOURNEY
SOC CAPABILITY
Log collection
Real-time correlation & detection analytics
Machine learning and behavior analytics
Proactive hunting
Security Orchestration, automation and response

Real-time Correlation and Detection Analytics

- Contextual understanding
- Powerful real-time correlation
- Quick threat detection and simplified SOC workflow
- Built-in security analytics delivers out-of-box visuals for security use cases



MICRO FOCUS


SECURITY OBJECTIVES
Machine Learning and Behavior Analytics
Act Faster
Avoid Disruptions
Work Smarter
Reach Further
Ensure Compliance
• "What are the unknowns"
• Rarity, anomaly, spikes
• "What's happening now"
• Set monitors
• Use cases library
• Real-time Workflow
• "I'll keep everything"
• Audit
• Compliance reports
ADAPTIVE SECURITY OPERATIONS JOURNEY
SOC CAPABILITY
Log collection
Real-time correlation & detection analytics
Machine learning and behavior analytics
Proactive hunting
Security Orchestration, automation and response

Machine Learning and Behavior Analytics

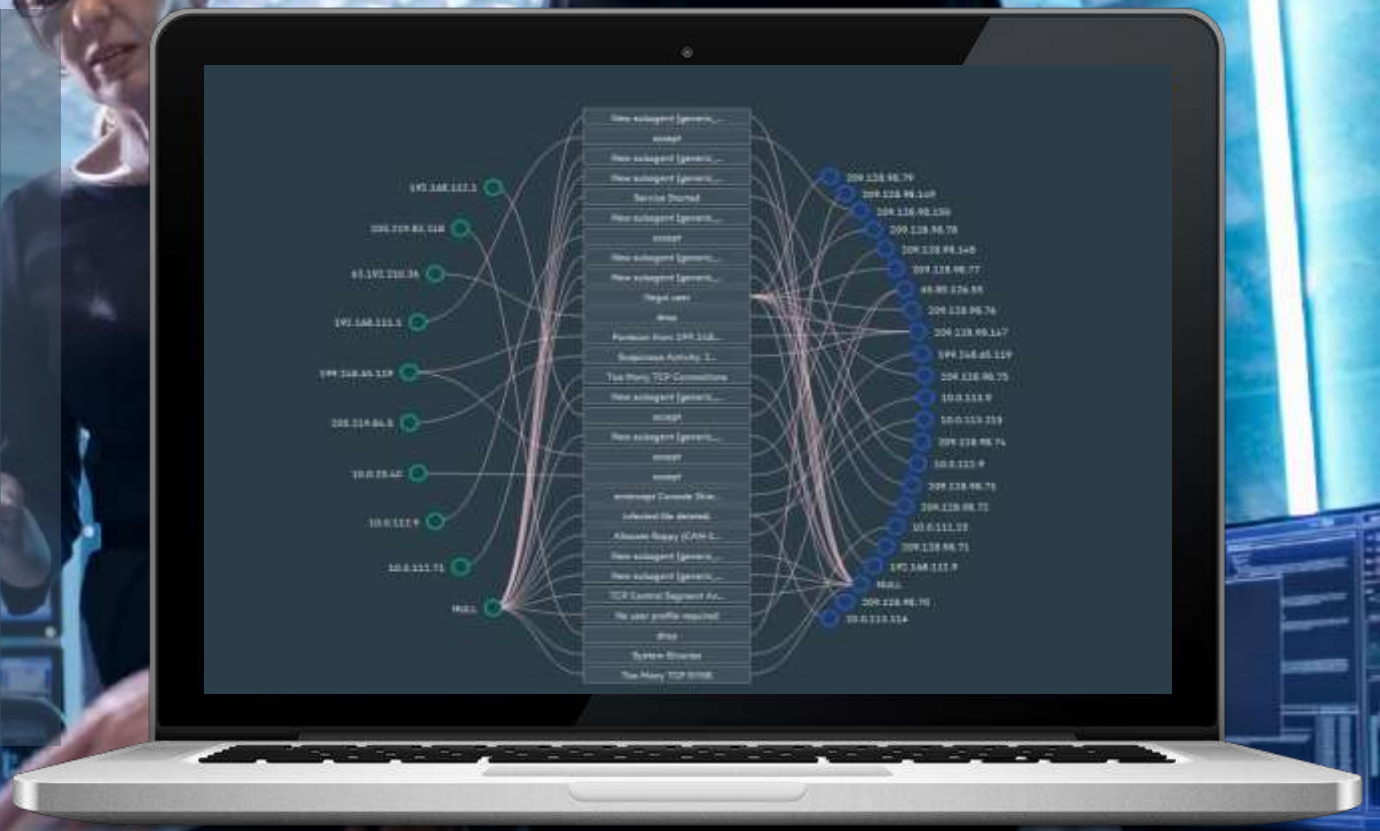
- Anomaly detection
- Threat and data modeling
- Machine learning and AI
- Rarity, patterns and spikes
- Algorithms and data science

MICRO FOCUS


SECURITY OBJECTIVES
Act Faster
Avoid Disruptions
Work Smarter
Reach Further
Ensure Compliance
Proactive Hunting
• "What is out there?"
• Analysis in Depth
• Information Fusion
• Threat Intelligence
• "What are the unknowns"
• Rarity, anomaly, spikes
• "What's happening now"
• Set monitors
• Use cases library
• Real-time Workflow
• "I'll keep everything"
• Audit
• Compliance reports
ADAPTIVE SECURITY OPERATIONS JOURNEY
SOC CAPABILITY
Log collection
Real-time correlation & detection analytics
Machine learning and behavior analytics
Proactive hunting
Security Orchestration, automation and response

Proactive Hunting

- Host and User Profiling
- DNS Analytics Capabilities
- Access data across security data lakes like Elastic and Hadoop
- Pre-defined visuals for security use cases remove guess work from the security hunting process
- Threat intel



MICRO FOCUS


SECURITY OBJECTIVES
Act Faster
Avoid Disruptions
Work Smarter
Reach Further
Ensure Compliance
Security Orchestration, Automation and Response
• "What action to take?
• Integrated SIRT workflow
• Automated actions
• "What is out there?"
• Analysis in Depth
• Information Fusion
• Threat Intelligence
• "What are the unknowns"
• Rarity, anomaly, spikes
• "What's happening now"
• Set monitors
• Use cases library
• Real-time Workflow
• "I'll keep everything"
• Audit
• Compliance reports
ADAPTIVE SECURITY OPERATIONS JOURNEY
SOC CAPABILITY
Log collection
Real-time correlation & detection analytics
Machine learning and behavior analytics
Proactive hunting
Security Orchestration, automation and response

Security Orchestration, Automation & Response

- Open API to integrate with devices and execute scripts
- Integrations with Micro Focus Operations Orchestration and Siemplify
- OOTB support to key SOAR providers

Analyst Productivity

300%

Increase in caseload capacity

Accelerated Response

70%

Average reduction in meantime to remediate -

MICRO FOCUS

ArcSight Command Center | Dashboards | Events | Reports | Cases | Applications | Administration | Stats | admin | Site Map

Active Channel - Main SOC Channel

Main SOC Channel

Start Time = 2017 April 13, Thursday 14:26:00 UTC-7 End Time = 2017 April 13, Thursday 14:57:00 UTC-7

Condition Summary | Priority Stats

Visualize Events

Channel Loaded

Total Events = 2773

Event List

View Details | Add to Case | Annotate | Mark As Reviewed | Customize

End Time	Name	Attacker Address	Event Annotation Stage	Target Address	Priority	Device Vendor	De
2017 April 13, Thursday 14:56:..	Suspicious URL	15.214.1.1	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	
2017 April 13, Thursday 14:56:..	Brute Force Login Attempts	16.157.255.1	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	
2017 April 13, Thursday 14:56:..	Malware infection detected	16.157.255.1	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	
2017 April 13, Thursday 14:56:..	Reconnaissance scan activity	34.57.225.73	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	
2017 April 13, Thursday 14:56:..	Malicious Tool Use Detected	24.15.25.123	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	
2017 April 13, Thursday 14:56:..	Suspicious URL	15.214.1.1	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	
2017 April 13, Thursday 14:56:..	Malware infection detected	16.157.255.1	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	
2017 April 13, Thursday 14:56:..	Malicious Tool Use Detected	24.15.25.123	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	
2017 April 13, Thursday 14:56:..	Brute Force Login Attempts	16.157.255.1	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	
2017 April 13, Thursday 14:56:..	High number of IDS Alerts for DoS	16.157.255.1	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	
2017 April 13, Thursday 14:56:..	Suspicious URL	15.214.1.1	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	
2017 April 13, Thursday 14:56:..	Reconnaissance scan activity	34.57.225.73	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	
2017 April 13, Thursday 14:56:..	Malicious Tool Use Detected	24.15.25.123	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	
2017 April 13, Thursday 14:56:..	High number of IDS Alerts for DoS	16.157.255.1	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	
2017 April 13, Thursday 14:56:..	Suspicious URL	15.214.1.1	<Resource URI="/All Stages/Que...	15.214.1.1	7	ArcSight	

MICRO FOCUS

Thank you.

www.microfocus.com/solutions/security