UEBA: Empowering the CISO

Mirco Rohr

Senior Enterprise Sales Engineering

July 25, 2019

LogRhythm
The Security Intelligence Company

What's On The CISO's Mind?

- CISOs care about outcomes that contribute to:
  - Safety - Resilient and defensible
  - Enablement of the business
  - Protection from a breach
  - Better and more efficient security operations
  - Achieving their security strategy

- CISOs have concerns about:
  - Duplication in capabilities
  - Gaps this product fills
  - Technology used
  - Total cost of ownership

An Effective Modern SOC

- Complete visibility
- Ability to answer questions
- Protect your assets
- Detect and respond to threats
- Compliance
- Instill confidence
- Cost appropriate staffing
- Provides business value
- Manageable and sustainable

The Value Of UEBA

- UEBA cuts across all of it
- Focused on behaviors, regardless of other protective and detective technology investments
- Bridges the gap with existing detection and response capabilities
- Easily integrated into existing SOC workflows
- Enables threat hunting in favor of reactive response

UEBA With Scenario *and* Anomaly Based Detection

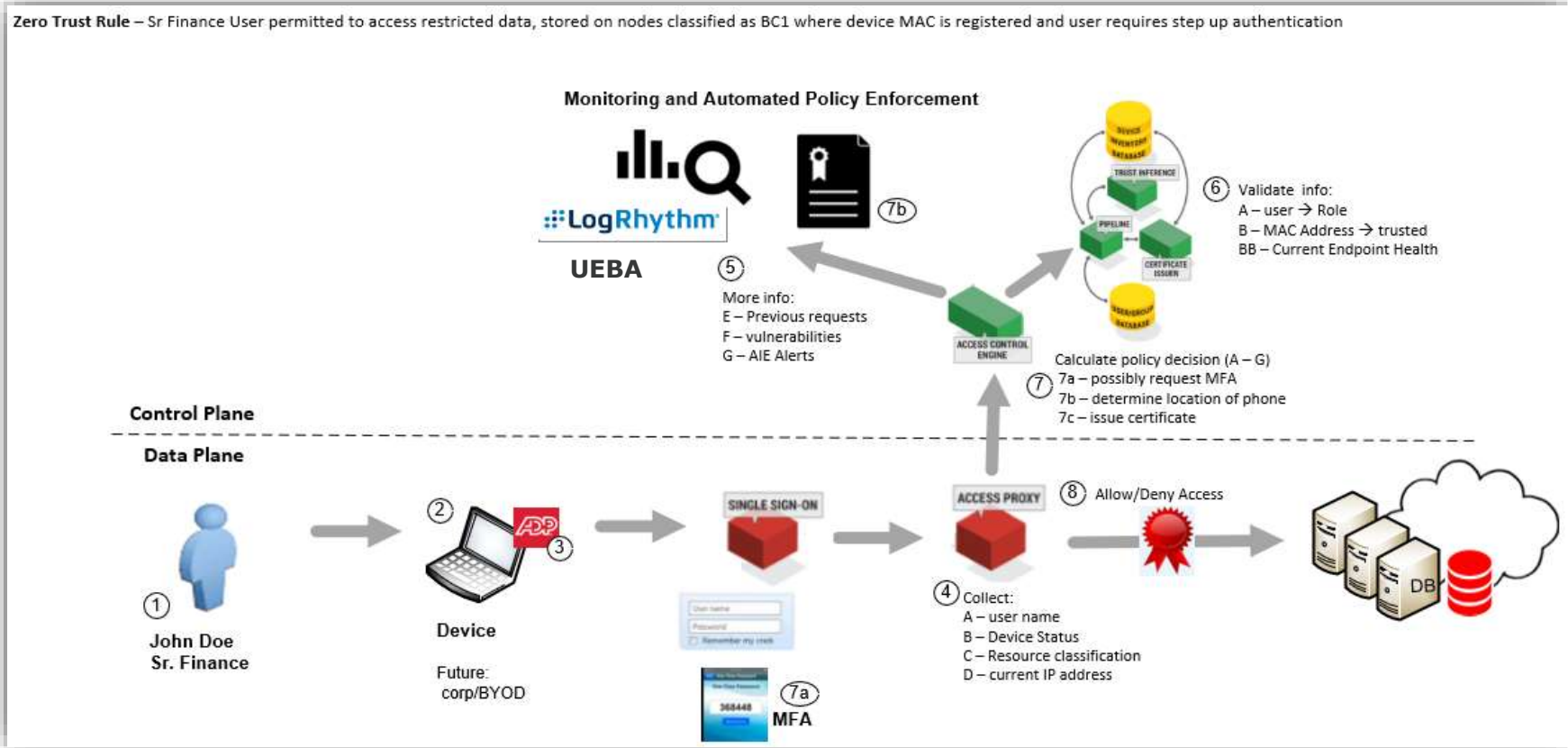
Scenario Based Detection

- Known attacker tactics, techniques, and procedures
  - Allows for detection without requiring specific IOC data (e.g. signatures)
  - Repeatable pattern for cyber attacks
  - Focused on behavior patterns of your adversaries
- Can leverage known indicators of compromise (IOCs)
  - Specific observables from artifacts
  - Shorter time to live
- Precise detection, alarming, and action-ability
- Does not require constant training of data

Anomaly Based Detection

- Known patterns or models of normal vs. not normal
  - Identifies activities that deviate in some way and by some amount
  - Baseline comparison
- Generates investigative leads
  - Enabled threat hunting
- Requires training of data as “normal” changes in many environments
- Critical when the attacker, patterns, intent, code or access, etc. are not publicly known or if the attacker is targeting your organization specifically

UEBA And IAM



UEBA And Cloud Security

- Data breaches
- Insufficient identity, credential, and access management
- Insecure interfaces (UI and API)
- System vulnerabilities
- Account hijacking
- Malicious insiders
- Advanced Persistent Threats
- Data loss
- Insufficient due diligence
- Abuse and nefarious use of cloud services
- Denial of Service
- Shared technology vulnerabilities

UEBA Directly Addresses

UEBA Enables

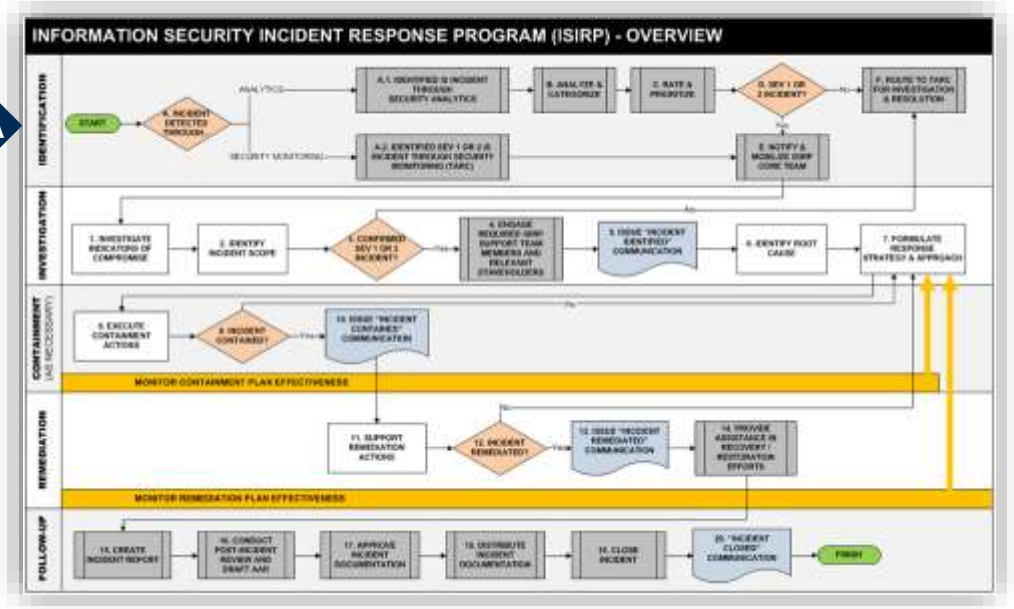
Credit: Cloud Security Alliance (CSA)

https://www.csoonline.com/article/3043030/the-dirty-dozen-12-top-cloud-security-threats.html

UEBA And Workflow Automation

- Enables fast identification
- Automates workflow via SmartResponse
- Identifies threat hunting starting points

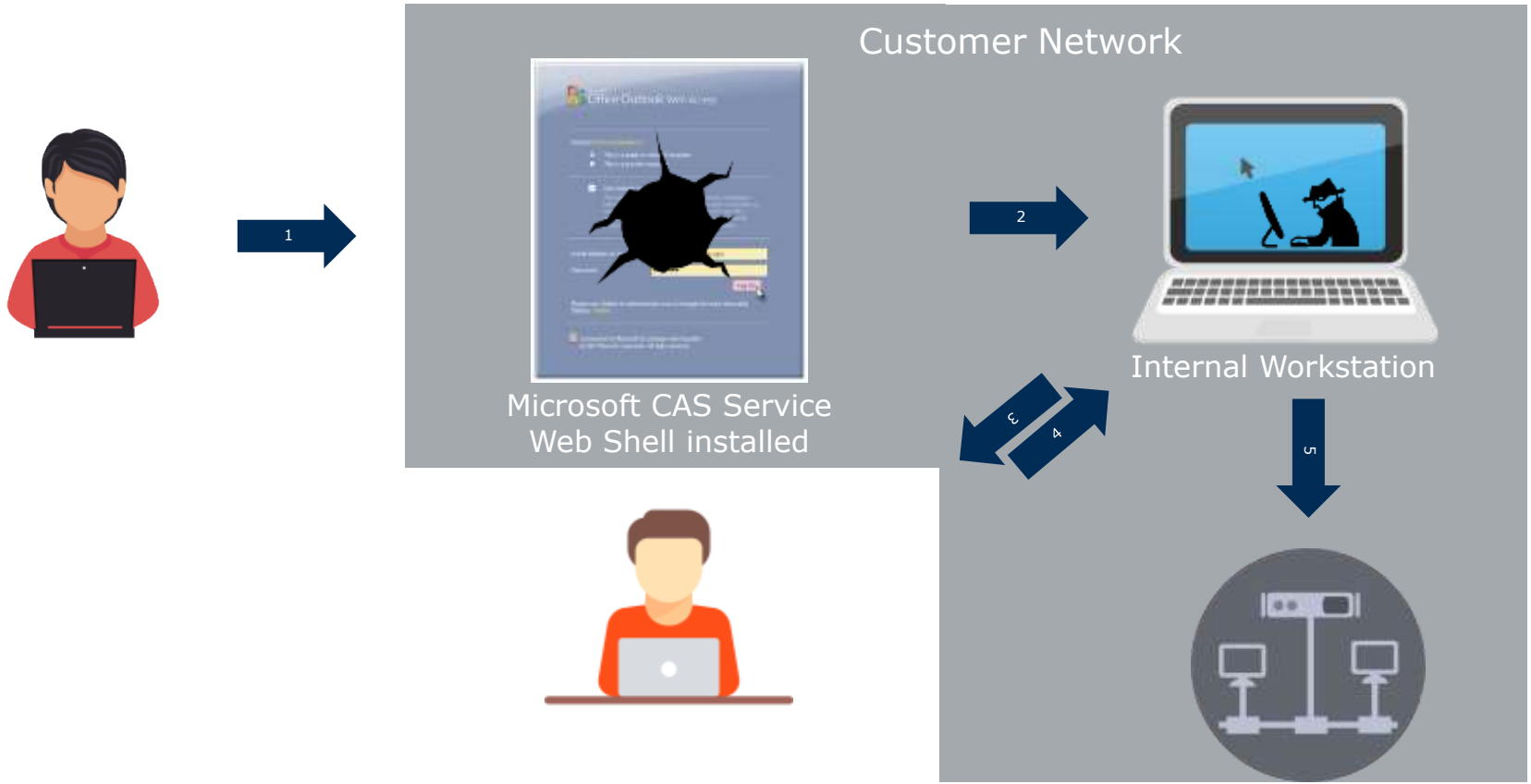
UEBA



UEBA In Practice

LogRhythm
The Security Intelligence Company

APT Compromise Of A Pharmaceutical



APT Compromise Of A Pharmaceutical

User Activity

- Remote IP address accesses OWA (7PM EST)
- User credentials supplied with an incorrect password
- Error redirect page had an installed web shell
- Lateral movement to internal user workstation
- Established backdoor on user workstation to second IP address
- Break in Action (11PM to 1230AM EST)
- Lateral movement to internal data stores
- Exfiltration of pharma research
- Clean up and disconnect (4AM EST)

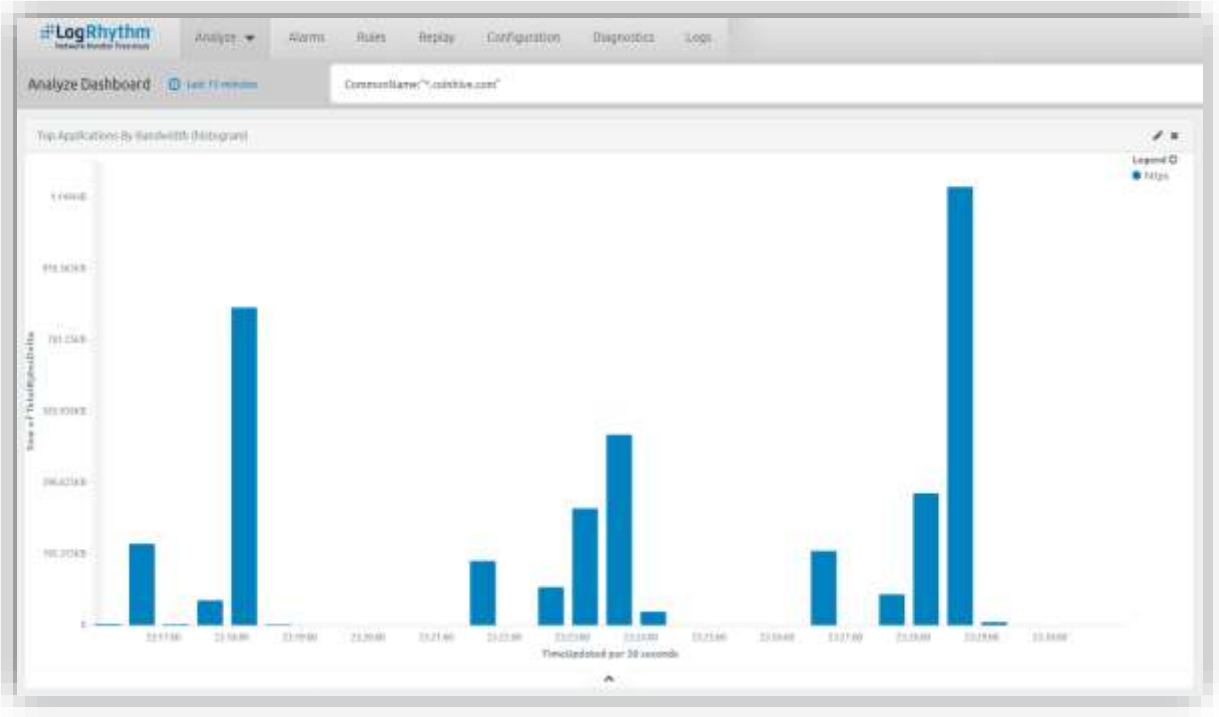
User Entity Behavior Analytics

- User Authentication location (unknown IP addresses that was never seen before) and time (7PM to 4AM)
- Single failed logon to OWA at the same time every day and no other activity at or near that time
- Compromised workstation used was not registered to the user that accessed it (domain administrator directly accessing)
- Credentials; accessing multiple disparate data stores from a single user workstation
- Proxy tunnel from user workstation to Internet; data transfers

Threat Hunting And Network Monitor

- NetMon is used for further validation

- Malicious activity is halted
- Machines are restored
- Employee is terminated
- Evil is thwarted



In Summary

- UEBA is a component of a platform, not a solution in and of itself
- UEBA enables the modern SoC
- UEBA thwarts malicious activity via scenario and machine learning
- UEBA speeds threat hunting
- UEBA enhances SoC workflow
- UEBA cuts across every aspect of an organizations technology
- UEBA drives efficiency.
- UEBA enables the CISO to achieve his or her goals

Questions?