RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: STR-W02

How to Detect and Stop Attacks as They Occur on a Limited Budget

John Allred

Senior Manager, Cybersecurity
EY
@jallred6

Guidelines

- No product recommendations
- No company mentions
  - If I slip up, don’t read anything into the mention
- People, technical capabilities and integration only

Why?

- Average time to detect an attack – hundreds of days
- High cost of a full remediation
- High cost of lost intellectual property
- High cost of business downtime
- Detect an attack sooner -> less cost
- Let’s get detection time down to 300 seconds

True story!

Red team attack

Another true story!

Interactive attackers breach a remote office, then move laterally

Capabilities to enable quick response

People

- Choose them well
- Train them well
- Rotate duties over time

Endpoint Telemetry

- More than event logs and Antivirus
- Fine details
- Searches against these fine details for suspicious behavior

Network monitoring

- Egress
- East-west
- For segments and endpoints without endpoint telemetry

Bring it all together

- SIEM for correlation and analysis
- Alerts from endpoint and network
  - Possibly raw endpoint telemetry as well
- Enriched and more data from other log sources
  - DNS, DHCP, Windows events, Firewall, Web Proxy

Bring it all together (continued)

- Other tools
  - Netflow analysis and analytics
  - User Behavior Analytics
- Alert when you haven’t heard from a data source for a time
- Priority alerts from critical devices and infrastructure

Antivirus/Next Gen Antivirus

- These product categories are merging
- Use them to block the commodity attacks, so your team can focus on the sophisticated attacks and anomalies that might indicate reconnaissance or an attack

Controls

- Application whitelist
- Network segment “lock”

People multipliers

- Let your team think about real attacks, and how to change architecture to prevent in the future
- Define normal for your environment
- Endpoint and network tools tuned -> increased signal/noise
- Consider outsourcing some analysis
- Automation
- Threat intel informs where and how to look

Cloud monitoring

- Often this is an extension of your corporate environment
- Where you can, treat cloud endpoints as “normal” endpoints
- Ingest application use, user activity, and security logs
- CASB logs

Challenges

- Opaque alerts (“There’s something bad, over there. Sorry, no details.”)
- Machine learning appears to be over-hyped

Put together a detection and response system that fits you

Some assembly and customization required!

Priorities

- People
- Endpoint
- SIEM
- Network

What to do in the next n days

- 30 days
  - Know your environment, and your visibility
  - Understand the surprises found
  - Present surprises to senior management, and get budget to fix, or an explicit acceptance of the business risk by the Executives and Board of Directors.
  - Review the capabilities of your team, and your hiring process
  - Compare Endpoint telemetry tools features; schedule demo
- 60 days
  - Evaluate one or more endpoint telemetry tools
- 90 days
  - Deploy endpoint telemetry tool
  - Test with purple team

Thank you!

Questions?

“Apply” Slide

- Bullet point here (see slides 5 – 8 for instructions)
- Bullet point here
- Bullet point here

RSA® Conference2019

RSAConference2019