



Jonathan Park
Summer 2024 Cybersecurity Intern

first look at

exabeam

the problem





one place for all* the data and/or activity within the organization

* that Cyber would care about:





* that Cyber would care about:



- ! System logins
(failed or successful)
- ! Unexpected geolocation
- ! Activity from new or
unrecognized devices
- ! File downloads
- ! Potentially malicious scripts
etc.

cyber kill chain





exabeam

tour



advantages



one place for all* the data
and/or activity within the
organization



get an immediate sense of most
eminent threats across the firm,
prioritize by highest risk



high customizability,
mold to fit workflows & risks
unique to Aristotle

advantages



one place for all* the data and/or activity within the organization



high customizability, mold to fit workflows & risks unique to Aristotle



get an immediate sense of most eminent threats across the firm, **prioritize by highest risk**



considerations



customizing takes time. lots of sorting through false positives/noisy alerts, upping risk scores for specific aspects, etc. in the short term

cyber kill chain




















- ! Scanning open ports
- ! Unusual amounts of traffic to web pages containing sensitive info
- ! Potentially malicious scripts
- ! Unusual file creation patterns
- ! System logins (failed or successful)
- ! Unusual application behavior
- ! Unusual outbound connections
- ! Unexpected geolocation
- ! Emails with suspicious attachments or links
- ! File downloads
- ! Known exploit patterns
- ! New services or scheduled tasks that match known backdoor behavior
- ! Activity from new or unrecognized devices
- ! Large data transfers
- ! Unusual file access patterns

What's next?



- | | |
|---|--|
|  Scanning open ports | |
|  Unusual amounts of traffic to web pages containing sensitive info |  File downloads |
|  Potentially malicious scripts |  Known exploit patterns |
|  Unusual file creation patterns |  New services or scheduled tasks that match known backdoor behavior |
|  System logins (failed or successful) |  Activity from new or unrecognized devices |
|  Unusual application behavior | |
|  Unusual outbound connections |  Large data transfers |
|  Unexpected geolocation |  Unusual file access patterns |
|  Emails with suspicious attachments or links | |

What's next?

Establish baseline

Update incident response

Metrics reporting

Pentesting

Training & documentation



- | | |
|---|--|
| ⚠ Scanning open ports | |
| ⚠ Unusual amounts of traffic to web pages containing sensitive info | ⚠ File downloads |
| ⚠ Potentially malicious scripts | ⚠ Known exploit patterns |
| ⚠ Unusual file creation patterns | ⚠ New services or scheduled tasks that match known backdoor behavior |
| ⚠ System logins (failed or successful) | ⚠ Activity from new or unrecognized devices |
| ⚠ Unusual application behavior | |
| ⚠ Unusual outbound connections | ⚠ Large data transfers |
| ⚠ Unexpected geolocation | ⚠ Unusual file access patterns |
| ⚠ Emails with suspicious attachments or links | |

Establish baseline

Update incident response

Metrics reporting

Pentesting

Training & documentation

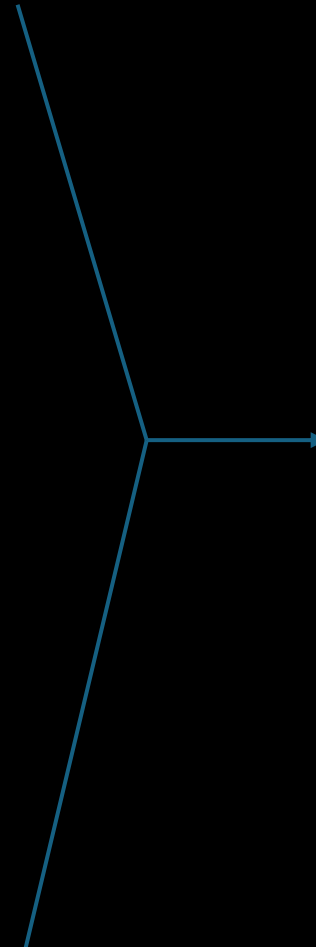


- ! Scanning open ports
- ! Unusual amounts of traffic to web pages containing sensitive info
- ! Potentially malicious scripts
- ! Unusual file creation patterns
- ! System logins (failed or successful)
- ! Unusual application behavior
- ! Unusual outbound connections
- ! Unexpected geolocation
- ! Emails with suspicious attachments or links
- ! File downloads
- ! Known exploit patterns
- ! New services or scheduled tasks that match known backdoor behavior
- ! Activity from new or unrecognized devices
- ! Large data transfers
- ! Unusual file access patterns





- ! Scanning open ports
- ! Unusual amounts of traffic to web pages containing sensitive info
- ! Potentially malicious scripts
- ! Unusual file creation patterns
- ! System logins (failed or successful)
- ! Unusual application behavior
- ! Unusual outbound connections
- ! Unexpected geolocation
- ! Emails with suspicious attachments or links
- ! File downloads
- ! Known exploit patterns
- ! New services or scheduled tasks that match known backdoor behavior
- ! Activity from new or unrecognized devices
- ! Large data transfers
- ! Unusual file access patterns



Establish baseline

Update incident response

Metrics reporting

Pentesting

Training & documentation



- | | |
|---|--|
| ⚠ Scanning open ports | |
| ⚠ Unusual amounts of traffic to web pages containing sensitive info | ⚠ File downloads |
| ⚠ Potentially malicious scripts | ⚠ Known exploit patterns |
| ⚠ Unusual file creation patterns | ⚠ New services or scheduled tasks that match known backdoor behavior |
| ⚠ System logins (failed or successful) | ⚠ Activity from new or unrecognized devices |
| ⚠ Unusual application behavior | ⚠ Large data transfers |
| ⚠ Unusual outbound connections | ⚠ Unusual file access patterns |
| ⚠ Unexpected geolocation | |
| ⚠ Emails with suspicious attachments or links | |

Establish baseline

Update incident response

Metrics reporting

Pentesting

Training & documentation

thank you!

Special thanks to:

Ryan Kaakaty
Ahmed El-Rayes
John Quan