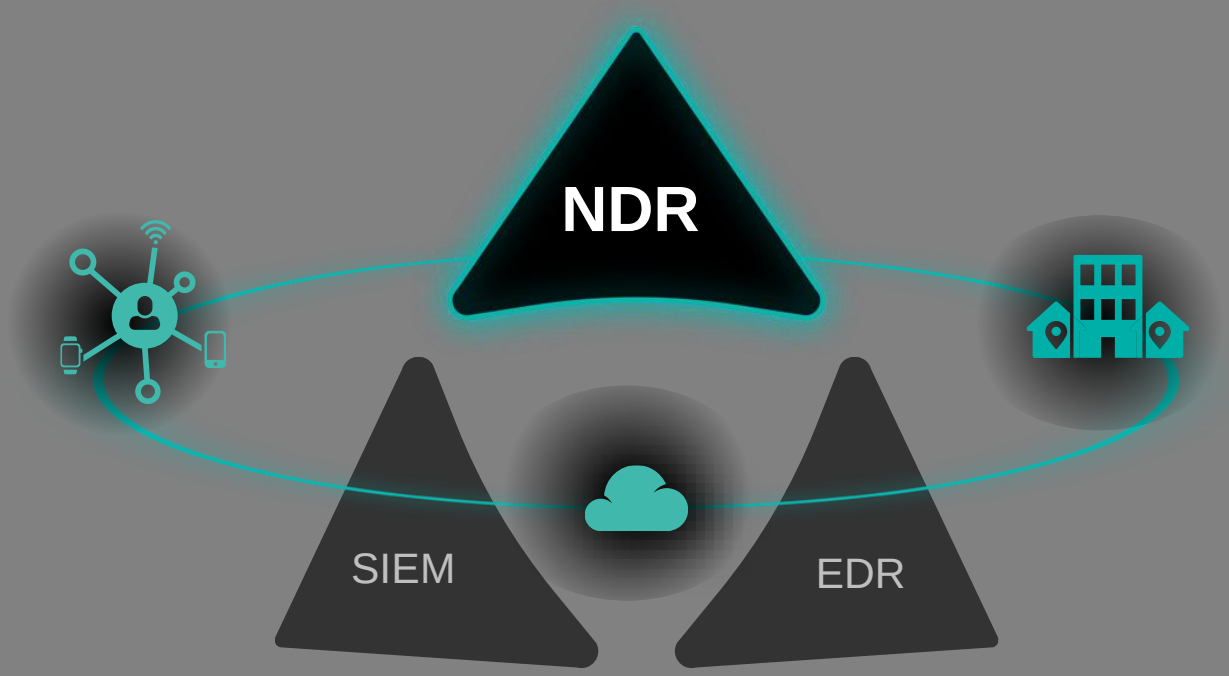
ExtraHop

Completing the Triad With Network Detection and Response

John Smith, Principal Security Engineer

ExtraHop Networks

Complete Visibility Across East-West and North-South



COMPLETE VISIBILITY

REAL-TIME DETECTION

INTELLIGENT RESPONSE

> Network-based detection tools got the highest levels of satisfaction when compared against other detection approaches.
>
> 2019 SANS SOC SURVEY RESULTS

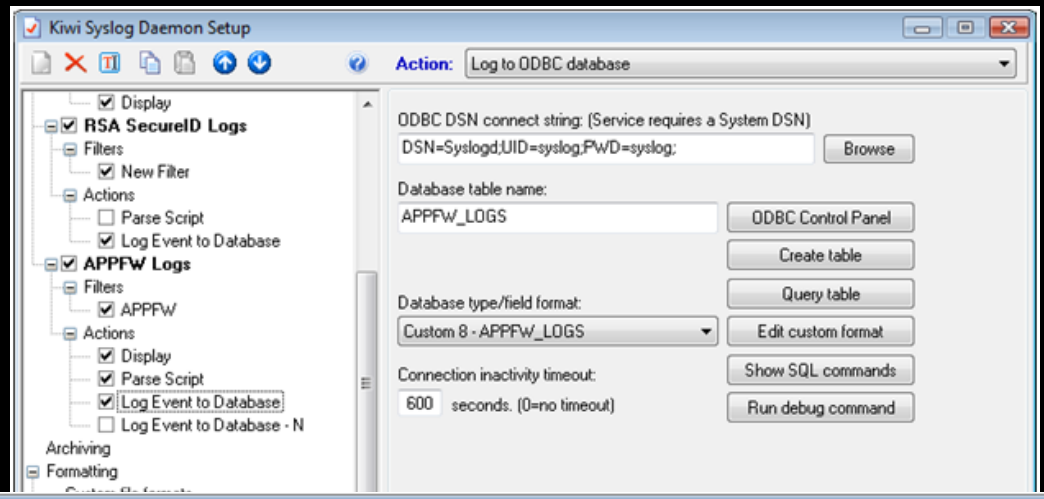
Security Information and Event Management(SIEM)

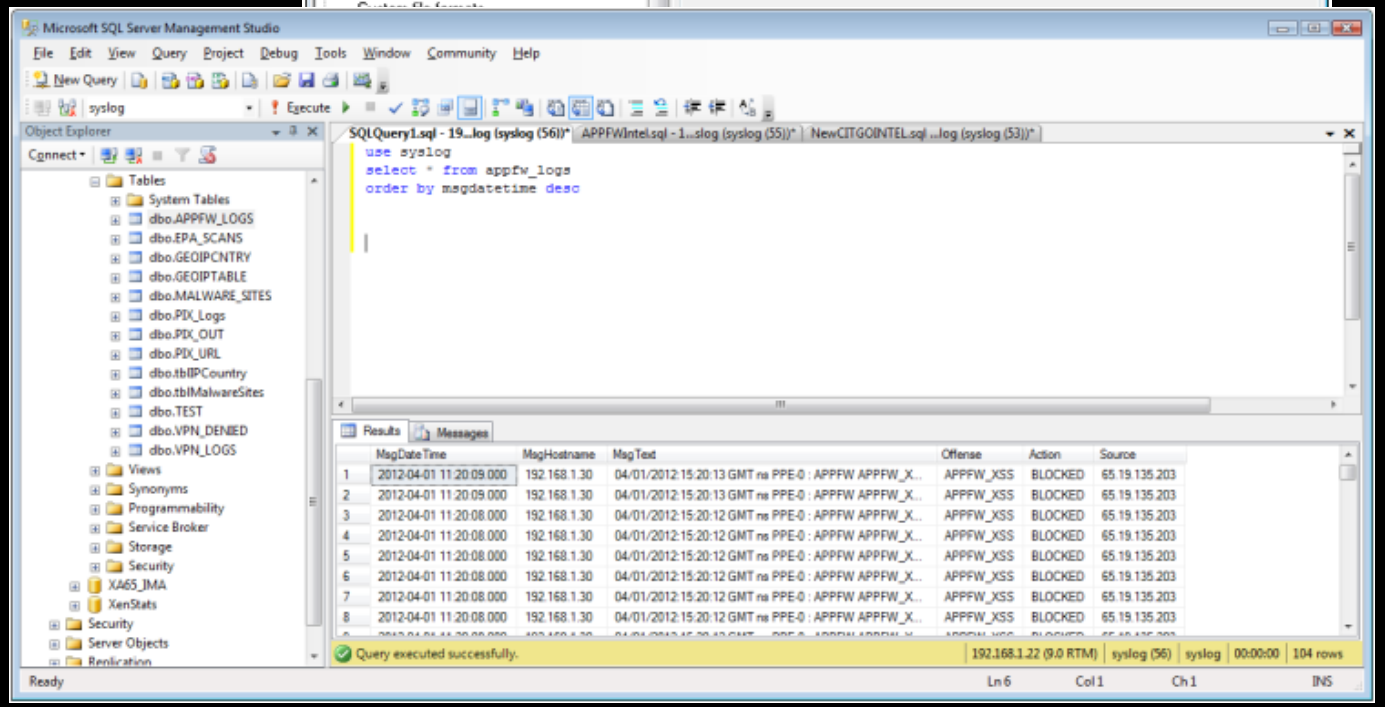
TRIED AND TRUE

- Born from Syslog and rSyslog
- Became very popular post Sarbanes-Oxley
- Has matured to become the focal point in most CSIRT program

LIMITATIONS

- Limited to what is programmed to ”log”
- Licensing can be costs can be prohibitive
- IOPS costs can be prohibitive
- Requires configuration and/or installation of forwarders
- Can be “un-configured” or “uninstalled”
- Logs/Events can be deleted or altered





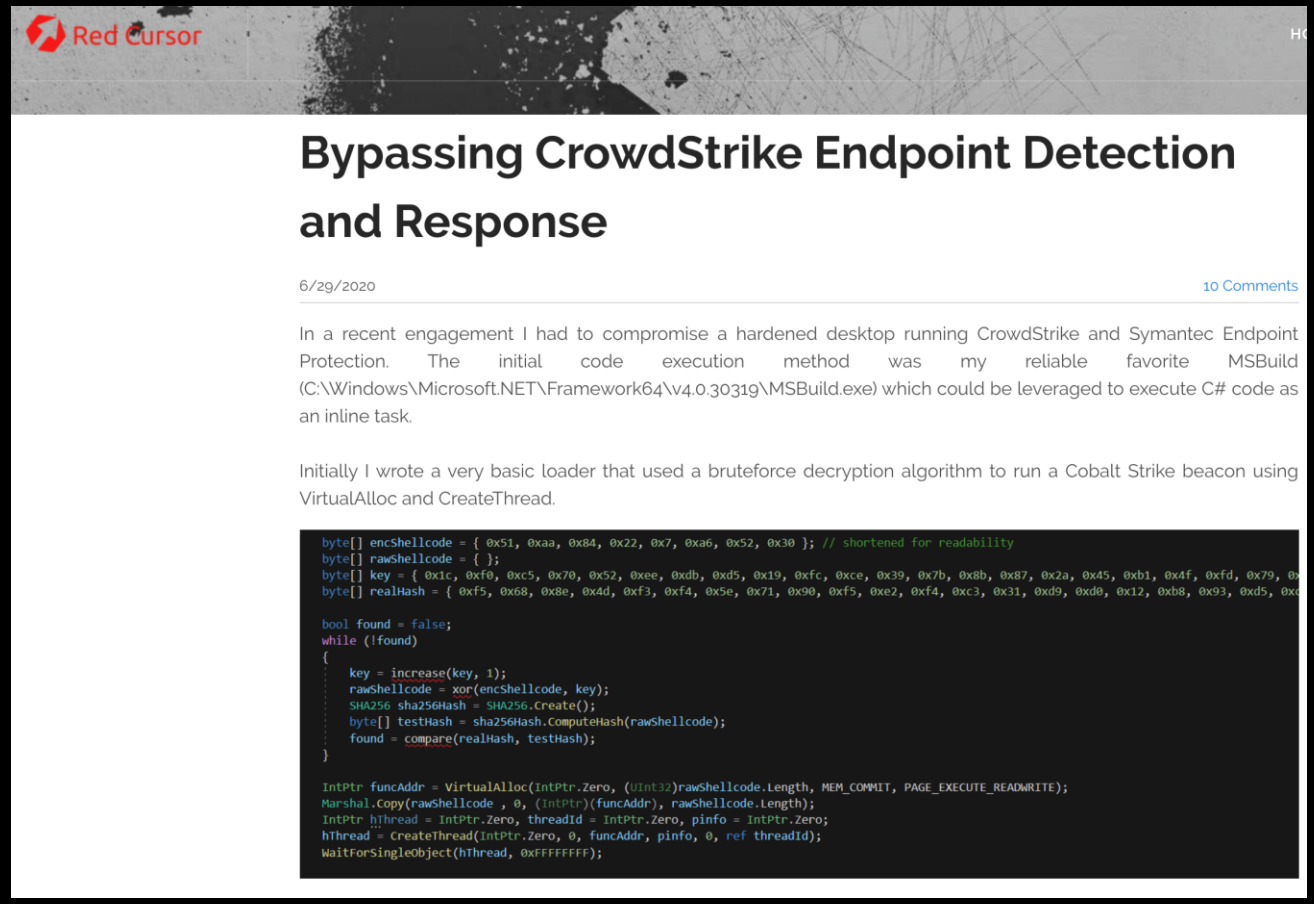
Endpoint Detection and Response (EDR)

TRIED AND TRUE

- Evolution from Antivirus to more behavioral detections
- Integration with Threat Intelligence Systems
- Provides process-level visibility
- More kinetic version of “R” as it will actually block malicious processes

LIMITATIONS

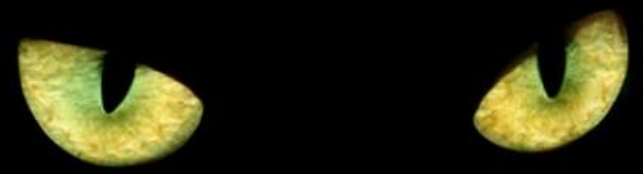
- Like Syslogs, an agent needs to be installed/configured
- Rapid endpoint provisioning makes ensuring deployment difficult
- Is limited to ”supported” operating systems and will require patching and updating
- Is often evaded/disabled by a crafty malware developer



What is NDR? (Network Detection and Response)

AND WHY DO I NEED IT?

- Wire/Network based Signal Intelligence
- Deployed using a SPAN/TAP to retrieve a traffic mirror
- Unlike IDS/IPS, it uses behavioral analytics, metadata and machine learning to inform on observed anomalies, threats and breaches
- Does not require large-scale Agent Implementation
- Does not require logging to be configured or the deployment of forwarders
- Cannot be manipulated, uninstalled or un-configured
- Operates in a “Covert” position whereby adversaries are NOT aware of its presence
- Positions SOC/Threat Hunters to flank adversaries who are unaware that they are being observed
- Taps into Network Metadata presenting several thousand tuples

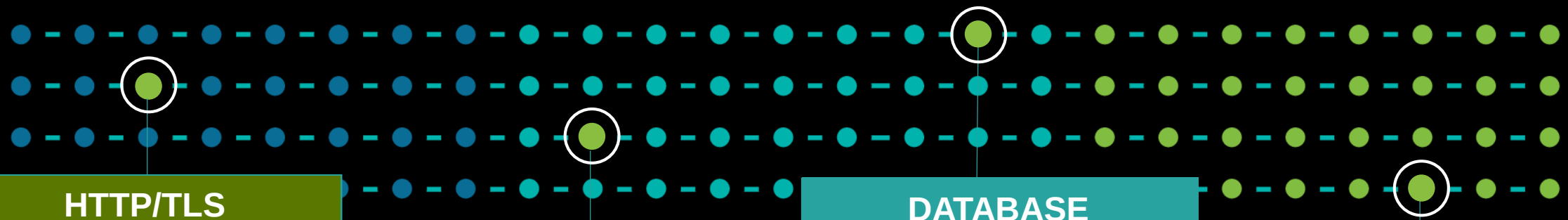


LIMITATIONS

- “R” is more API driven
- Cannot directly act against a bad actor
- Data Fidelity (SPAN/TAP)
- Cannot provide Process Information (Hashes)

STREAM PROCESSING: ANALYZING THE IMPORTANT METADATA

IT TEAMS DON'T LACK DATA, IT TEAMS LACK *INSIGHTS*



HTTP/TLS

- 121.35.232.13 → 192.168.1.3:80
- https://vpn.extrahop.com/login
- SQLMAP User Agent
- **Encoded POSH Payloads**
- HTTP POST webshell.php
- Cookie: …..
- UserName: john_smith
- ThreatIntel Matches
- User agent: Firefox53/ Windows10
- POSH JA3 going to raw.githubusercontent.com

CIFS/SMB

- Share: \\dc1\ipc$:Samr
- File: \\WS1\Desktop**a.ppt.encrypted**
- Method: WRITE
- Non Sysvol Traffic on DCs
- PSEXEC Activity
- Ransomware Activity
- UserName: john_smith

DATABASE

- 192.168.23.5 → 192.168.25.8:1521
- User: **sa**
- Query: select * from accounts
- Authentication failures followed by Successful queries
- Data Exfiltration: 102G to external IP
- Network Transfer Time: 0.5 ms
- Error: **ORA-00942 table or view does not exist**

KERBEROS

- 192.168.23.2 → 10.1.3.5:88
- User: Golden Ticket IDs
- Unusual Login Times
- Honey Token Accounts
- Misuse of Service Accounts
- Pass-the-Hash activity
- Password Changes at 2AM!!
- Error: **KDC_ERR_CLIENT_REVOKED**

The Cybersecurity Triad (Key functions of all three solutions)

SYSLOG

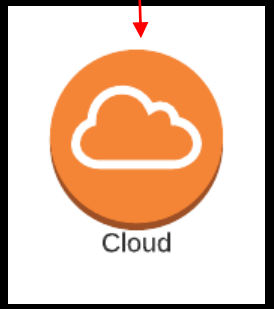
- Collect Logs from agents and devices
- Writes them to disk
- Extracts Context
  - Mashup (CTI)
  - ML Interrogation
  - Querying Logs
- Provides Investigation
- Provides Detections and Alerts

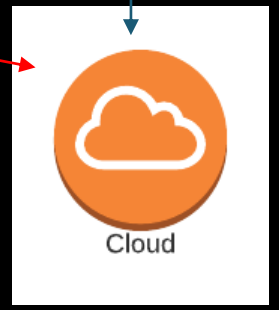
Reveal(X) NDR

- Passively listens on the network
- Evaluates metadata in microseconds
- Extracts Context in flight
  - Mashup
  - Pre-Defined Criteria
  - API Calls
- Extracts Context (ML)
  - Predictive Modeling
  - Group Clustering
  - Peer Grouping
- Integrate with Sec Portfolio
  - SOAR
  - SIEM
  - EDR
  - REST API

EDR

- Installed on an operating system
- Leverages Cloud based Machine Learning
- Extracts Context
  - Behavioral ML
  - Threat Intelligence
  - Process/Hash Level Metrics
- Blocks and/or quarantines systems and processes





Denotes the need to install or configure agents/forwarders/logging

Example: Phishing URI and Payload

SYSLOG

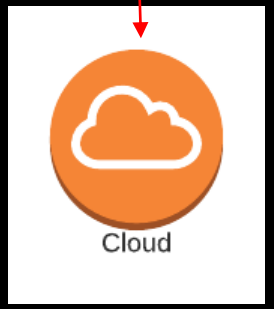
- Host
- Issuer
- Subject
- JA3
- Cipher
- Certificate Date Information
- ClientIP
- ServerIP

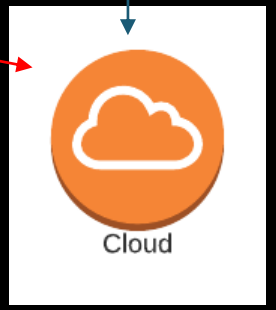
Reveal(X) NDR

- Host
- Issuer
- Subject
- JA3
- Cipher
- Certificate Date Information
- ClientIP
- ServerIP
- Server Geo Location
- SelfSigned (Y/N)
- Threat Intelligence Match (Y/N)
- *Does the Host Info match your Namespace?
- If decrypted will show Payload, user-agent, content-type, etc

EDR

- Waits until Payload is Downloaded
- When the Process starts the information is sent to the Cloud
- Based on The Information the process is quarantined or allowed to continue





Denotes the need to install or configure agents/forwarders/logging

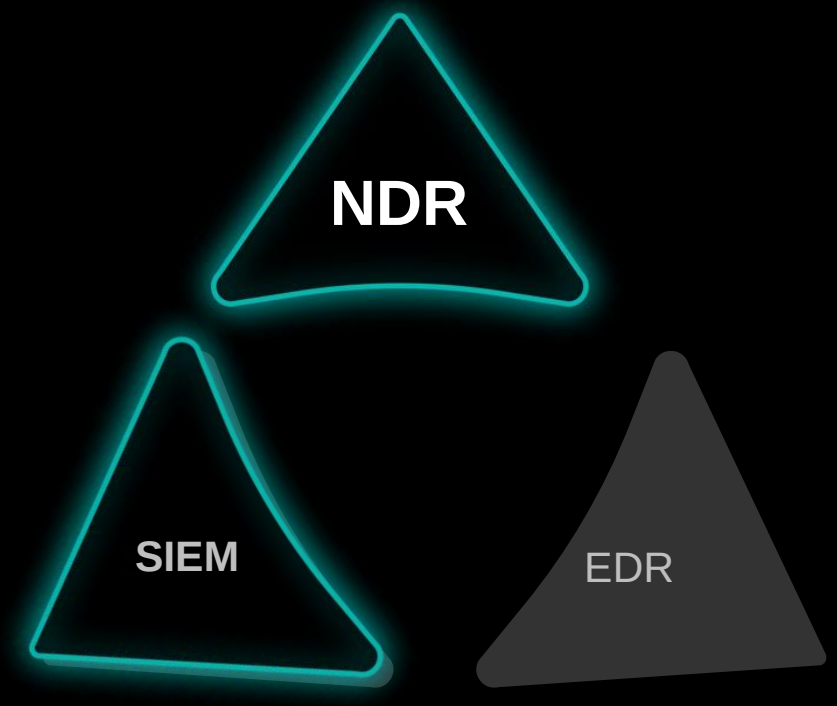
Using NDR and the SIEM (Better Together!)

NDR AUGMENTS YOUR SIEM

- Providing Visibility and Logging for IoT Devices
- Can alert when logging has been shut off
- Is still watching WHEN logging has been shut off
- Makes metadata off the wire directly available for SIEM integration
- Sets Context in real-time vs. writing to disk, reading from disk, THEN setting context

NDR IMPROVES YOUR SIEM

- Pre-Define Logging Conditions
  - Cert Issuer is LE and SNI matches your namespace
  - DNS Surveillance for malicious TLDs
  - Pull User IDs from decrypted Payloads and provide Geo-tracking of Teleworkers



Case Study (Making the SIEM Better: Malicious TLD Surveillance)

MONITOR MALICIOUS TLDS

- Customer wanted to monitor suspicious Top Level Domains
- Was using Splunk as the back end SIEM
- During peak business DNS traffic was over 2000 EPS

CHALLENGES

- Monitoring DNS is noisy (over 2000 EPS)
- Queries took a long time, even on hot storage
- IOPS and Storage costs were very high
- Deluge of records resulted in decreased efficacy of the endeavor altogether

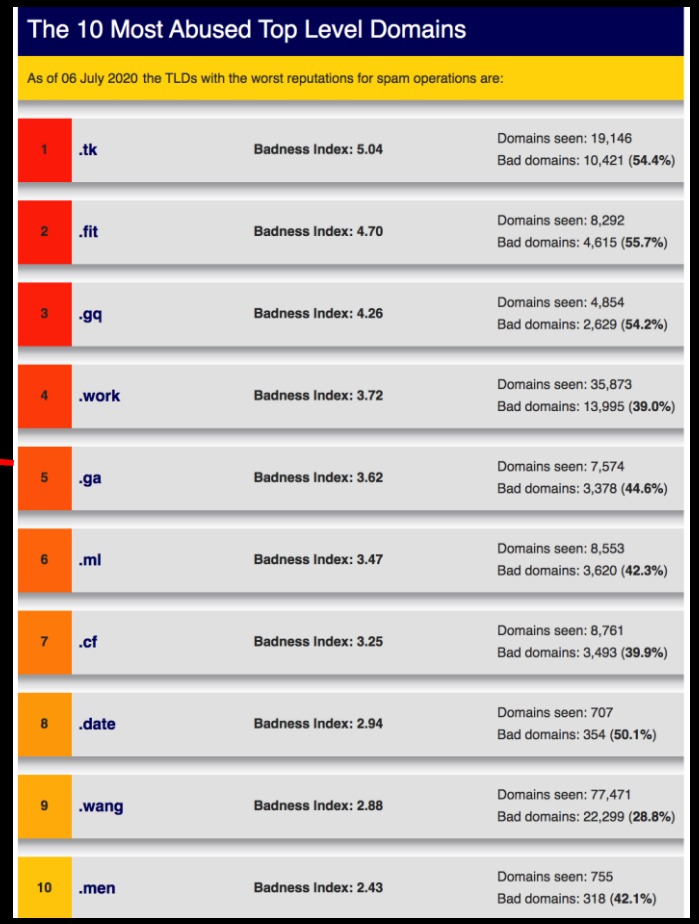
Making the SIEM Better: Enter Reveal(x) NDR

SOLUTION

- Pre-Define Malicious TLDs
- Send ONLY DNS records matching those conditions to the SIEM
- Added additional surveillance for namespace matching the customers (Phishing attempts)

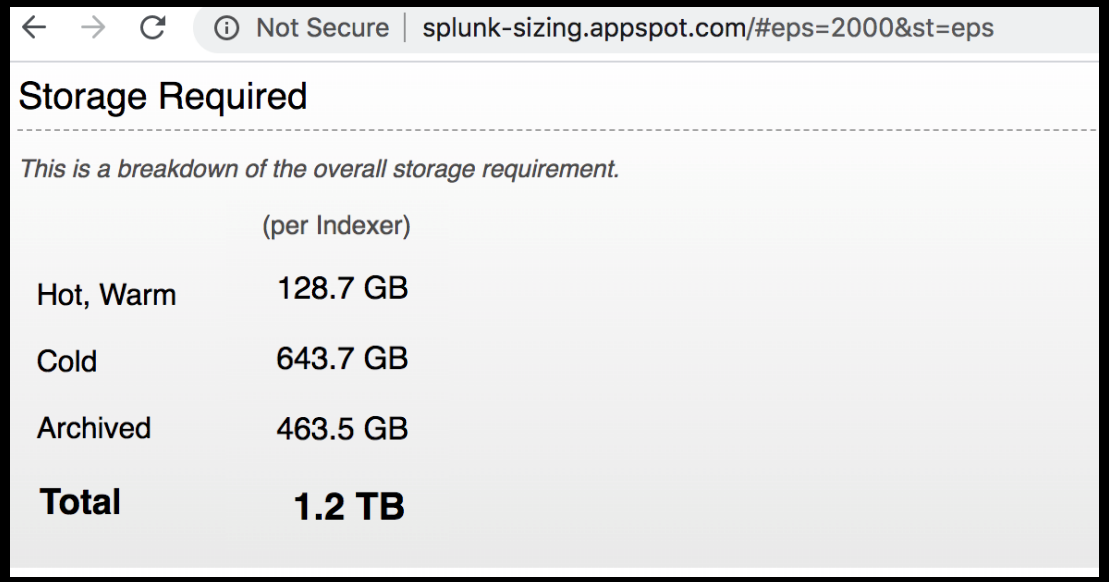
```
var i,
s,
maldns = [
          'ru', 'cn','tz','ua','by','kz','ir','iq','am','ge','tj','az','uz',
          'kg','rs','fit','tm','gq','work','review','kim','men','date',
          'party','tk','ml','ga','cf','ryukyu','wang'
         ]

len = maldns.length
domain = query.split(".").reverse()[0];
qdn = query.split(".").reverse()[1] + '.'+domain;
for(i = 0; i<len;++i) {
    if (domain === maldns[i]) {
        Remote.Syslog('splunk').emerg(JSON.stringify(DNS.record))
    }
```



Making the SIEM Better: Enter Reveal(x) NDR

WITHOUT NDR



USING NDR

- EPS went from 2000+ to less than 1 EPS
- Massive savings in Licensing and IOPS costs
- Added additional surveillance for namespace matching the customers (Phishing attempts)
- Increased Intelligence yield by several hundred orders of magnitude

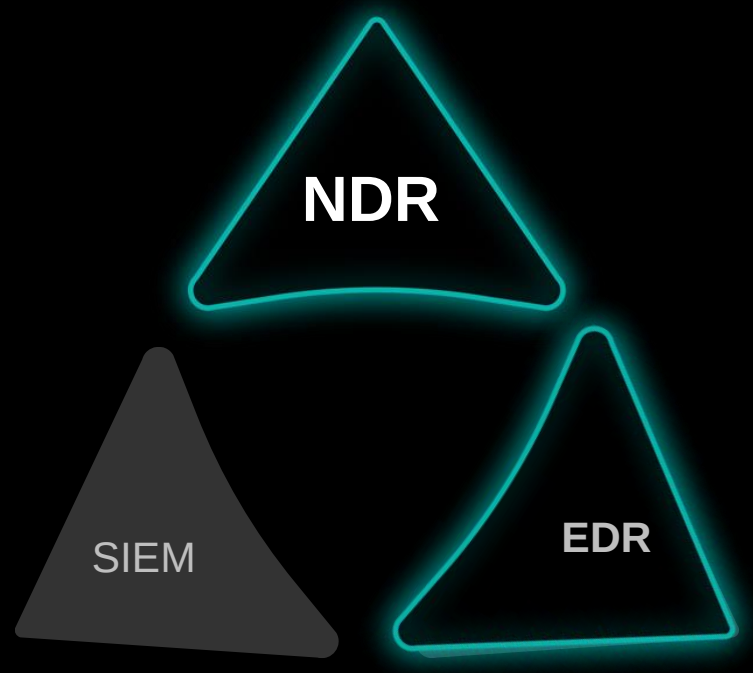
Using NDR and EDR (Better Together!)

NDR AUGMENTS YOUR EDR

- Providing Visibility into IoT Devices
- Can use API to ‘shun’ unmanaged devices
- Can create a map of EDR Traffic by CIDR block to show gaps in EDR coverage
- Makes metadata off the wire directly available to Falcon, Cloud based intelligence
- Sets Context in real-time vs. writing to disk, reading from disk, THEN setting context
- Can leverage Threat Intelligence

NDR IMPROVES YOUR EDR

- Network based Detections can use API to quarantine systems
- Pre-Defined metadata can be sent to Falcon API or other Cloud based solutions
- Packet Metadata and PCAPs can be made readily available



Case Study (Making the EDR Better: Breach Response)

RYUK THROW DOWN!!!!

- Healthcare provider had been hit with RYUK ransomware
- EDR Solution had been evaded and in many cases disabled/removed
- Cyber Response Team from Cyber Insurance Provider responded
- Endpoint-Driven Resolution was put into place

CHALLENGES

- There was a lack of visibility into which systems were infected
- The Response team ONLY had visibility into systems with deployed agents
- The Malware was using a very opaque SSL Channel to communicate
- VERY large gap in understanding the environment on the part of the 3rd party response team

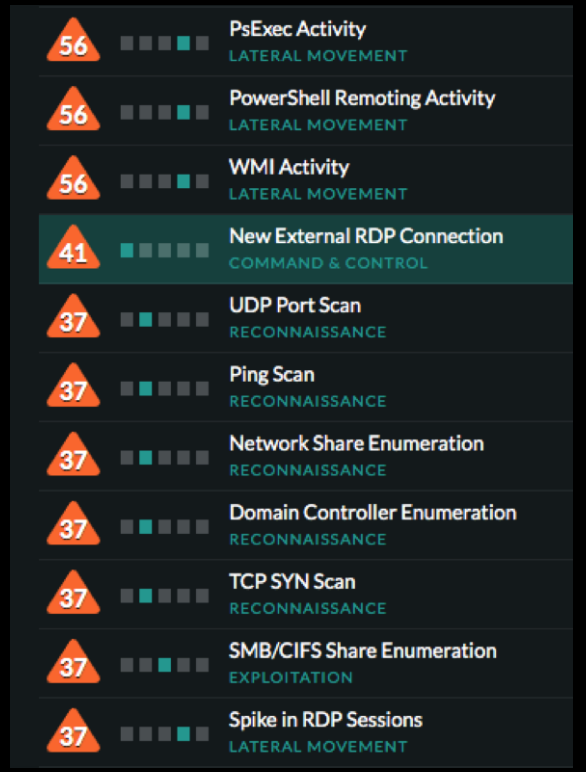
Reveal(x) NDR Detections and Observations

DETECTIONS

- Reveal(x) Detected Ransomware Activity
- CIFS/SMB Brute Force and Enumeration
- CIFS/SMB User Session Enumeration and High File Reads
- PSEXEC Activity
- POSH Remoting Activity

INVESTIGATIVE FINDINGS

- Their Active Directory Domain namespace had been externally registered by a nefarious registrar
- IAM traffic was going to the external malicious IP
- Emotet/Trickbot Infestation deploying the RYUK payload
- Several “Orphaned HTTP Posts” to malicious external IPs



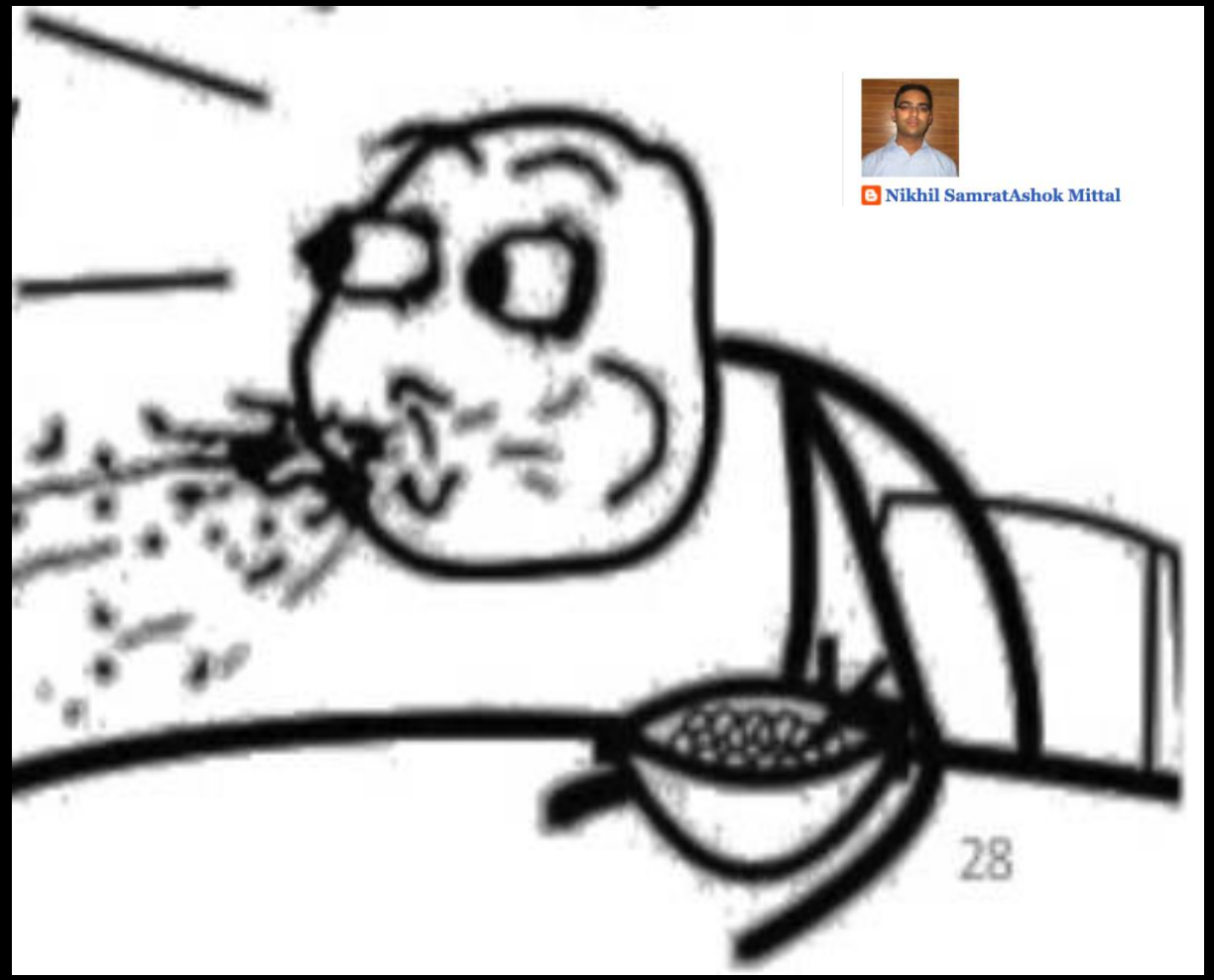
Investigative Findings (Continued)

Emotet/Trickbot Used to deploy the RYUK payload

- VERY suspicious SSL Characteristics
  - No HOST SNI, Cert Subject or Cert Issuer
  - Certificate was less than 48 hours old
  - Certificate was SELF SIGNED!!
  - Addresses, JA3s, etc were NOT on any blacklists

Noted Orphaned HTTP POSTS

- No preceding GETs
- Horrific payload data
  - Usernames/Passwords
  - SSH Key information
  - VNC Information
  - OS Patch Level
  - Current Running Processes
  - EDR Client Info
  - Binary Payloads
  - OpenVPN Passwords
  - ALL sites with the strings (/auth|login|logon/i)



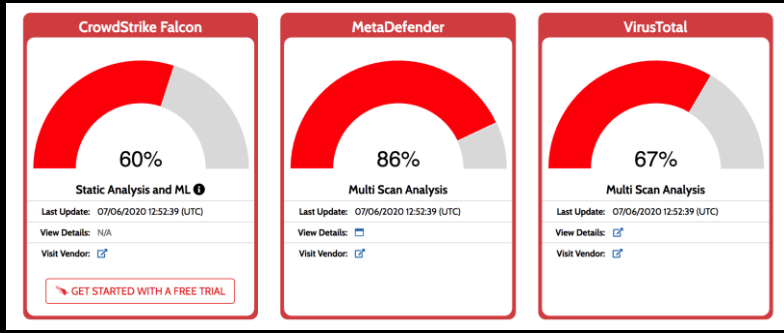
During the Response: (Working with EDR vendor)

Provide Visibility into what their current EDR coverage was

CIDR Block	Number of EDR Agents	Total Active Nodes
10.48.66.0	166	205
10.48.62.0	188	200
10.33.48.0	16	198
10.0.18.0	137	188
172.16.83.0	41	206

Painting Targets for Endpoint Detection and ~~Response~~ REVENGE!

- Malware was copying a file called minirev.exe
- All systems copying the file had EDR disabled
- Provided EDR team a list of systems engaged in copying the minirev.exe file
- Provided EDR team a list of systems minirev.exe had been copied to.



Conclusion: Apply what you have learned

LEAD WITH NDR

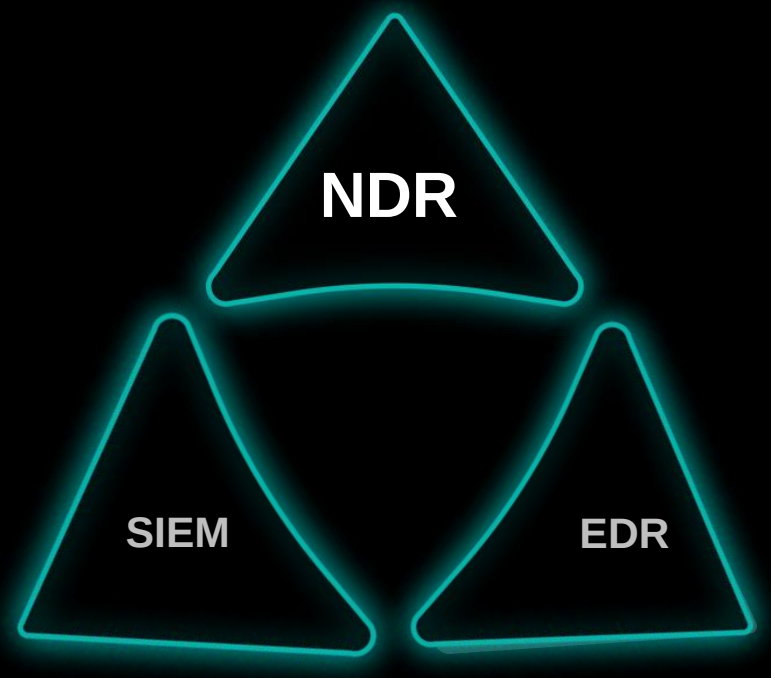
- No agents/forwarders to install or configure
- Only prerequisite is an IP Address (IoT, Unmanaged Systems)
- Several thousand sources of intelligence in Network Metadata
- Ultimate source of truth
- Covert posture (adversary can't see you but you can see them)

IMPROVE/AUGMENT SIEM

- If it doesn't log….it does now (IoT,etc)
- Higher Intelligence Yield
- Higher Fidelity Messages

IMPROVE/AUGMENT EDR

- Paint digital targets
- Shun unmanaged devices
- Cover for each other
  - Find gaps in EDR coverage
  - Gives NDR a hammer to swing when we see something



Thank you!!

Questions?

Questions and Next Steps