Who’s Watching Your Network?

Managed Detection and Response

Presenters:

Tom Callahan
Director of Operations, MDR
ControlScan

Mark Carl
CEO
ControlScan

CONEXXUS
solve forward

Agenda

- Housekeeping
- Presenters
- About Conexxus
- Presentation
- Q&A

Housekeeping

This webinar is being recorded and will be made available in approximately 30 days.

- YouTube (youtube.com/conexxusonline)
- Website Link (conexxus.org)

Slide Deck

- Survey Link – Presentation provided at end

Participants

- Ask questions via webinar interface.
- Please, no vendor specific questions.

Email: **info@conexxus.org**

Presenters

Conexxus Host

Allie Russell
Conexxus
arussell@conexxus.org

Jenny Bullard
Conexxus
jbullard@conexxus.org

Moderator

Mark Carl
Vice Chair, Data Security Committee
CEO, ControlScan
mcarl@controlscan.com

Speaker

Tom Callahan
Director of Operations, MDR
ControlScan
tcallahan@controlscan.com

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set standards…
  - Data exchange
  - Security
  - Mobile commerce
- We provide vision
  - Identify emerging tech/trends
- We advocate for our industry
  - Technology is policy

2019 Conexxus Webinar Schedule*

Month/Date	Webinar Title	Speaker	Company
January 2019	Managed Detection and Response	Tom Callahan Mark Carl	ControlScan
February 2019	PCI DSS for Petro Merchants	Elizabeth Terry	PCI SSC
March 2019	Protecting Your Stores and Main Stores from Data Security & Ransomware Attacks	TBD	Acumera
April 2019	Don't get Phished! Train Your Employees to Avoid Ransomware	Geoffrey Vaughan Ed Adams	Security Innovation
May 2019	Firewall compliance! The basics, the benefits, and the security	Simon Gamble	Mako Networks
June 2019	TBD	David Ezell Linda Toth	Conexxus Conexxus

CONEXXUS
solve forward

Conexxus thanks our 2018 Annual Diamond Sponsors!

mSHIFT. Relevant. Mobile. Solutions.

Stuzo

Diebold Nixdorf

wex

HUGHES An EchoStar Company

GILBARCO VEEDER-ROOT

Cybera Simplify Security and Networks

SECURITY INNOVATION

CONEXXUS solve forward

Presenters

Mark Carl
CEO
ControlScan

Tom Callahan
Director of Operations, MDR
ControlScan

CONEXXUS
solve forward

Threat Landscape – 2018

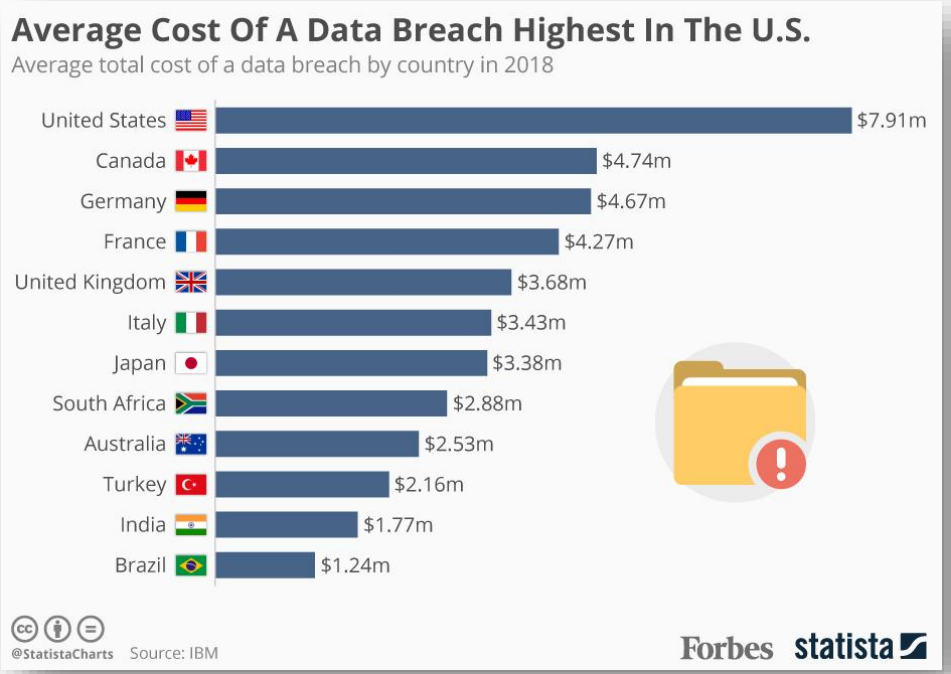
- 53,000 security incidents
- 2,200 reported data breaches
- 70% of breaches took longer than 3 months to discover
- 90% of retail breaches were through POS systems
- 20% of all breaches started through email phishing

Sources:

- https://www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#1e1984132f37
- https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

CONEXXUS
solve forward

Threat Landscape – 2018



- Average cost of a breach in the U.S. is $7.91 million
  - $148 per data record!

Source:
https://www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#1e1984132f37

CONEXXUS
solve forward

Threat Landscape – 2018

- **Phishing is the #1 entry mechanism to an organization.**
  - 16 minutes on average to the first click of phishing campaign
  - 16 minutes from launch to possible credential theft
  - 4% of people will click and submit credentials or download malware
- It only takes 1 person to cripple your systems!
- 49% of malware delivered through email.
  - Ransomware #1 payload, quickly decimating companies through file encryption.
- Unpatched systems, older systems lead to quick lateral movement.

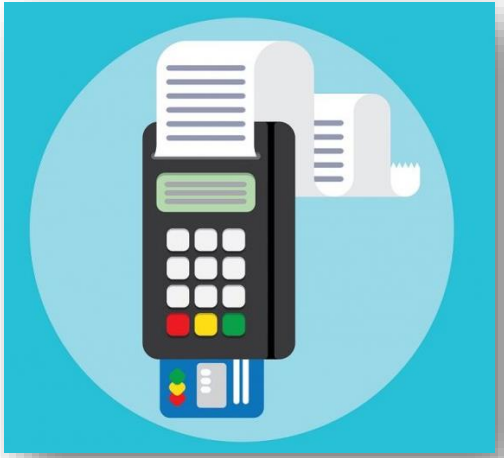
Sources:

- https://www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#1e1984132f37
- https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

CONEXXUS
solve forward

Threat Landscape – 2018

- 90% of retail breaches started at the POS System.
  - Controllers and terminals are high targets.
- Research shows you are 100 times more likely to be targeted if you have a POS system.
- POS systems are weak, and easy to exploit
  - Often running older and unpatched or unsupported operating systems
  - Often contain default or easily guessable passwords to privileged accounts
- External access for reporting without protections creates a major security hole.
  - Huge data source
  - Hundreds to hundreds of thousands of credit cards per day
- Lack of breach detection
- Most detections occurring through common point of purchase or law enforcement. Most retail stores never know until that point.



Sources:

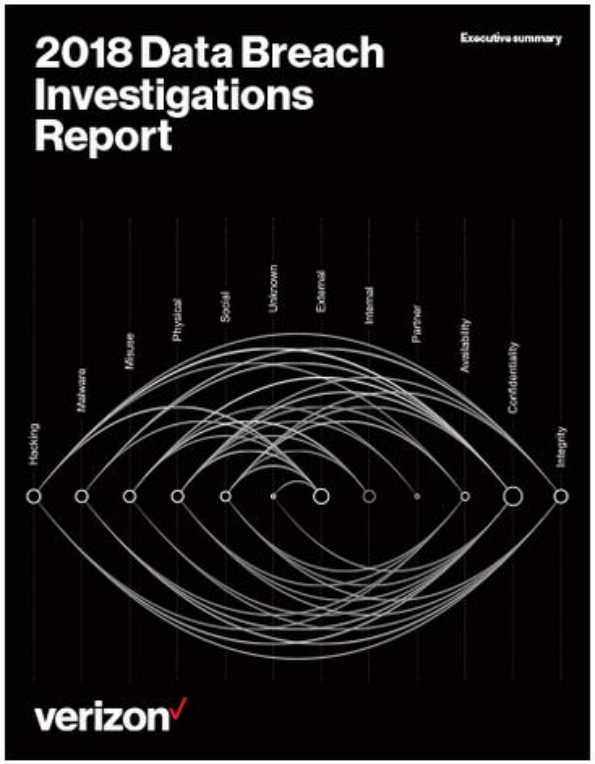
- https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

Modern Threat Landscape

“**Protecting your good name comes down to two things: defense and response**.

You should build defenses that are strong enough to send cybercriminals in the direction of an easier target. But no defense is 100% effective. Should an attacker get through, you need to be prepared to respond quickly and effectively.”

– Verizon 2018 Data Beach Investigation Report



CONEXXUS
solve forward

Managed Who and What?

- What is Managed Detection and Response (MDR)?
- Why does my company or organization need MDR?
- What about my existing security tools and team?

Managed Detection

What is Managed Detection?

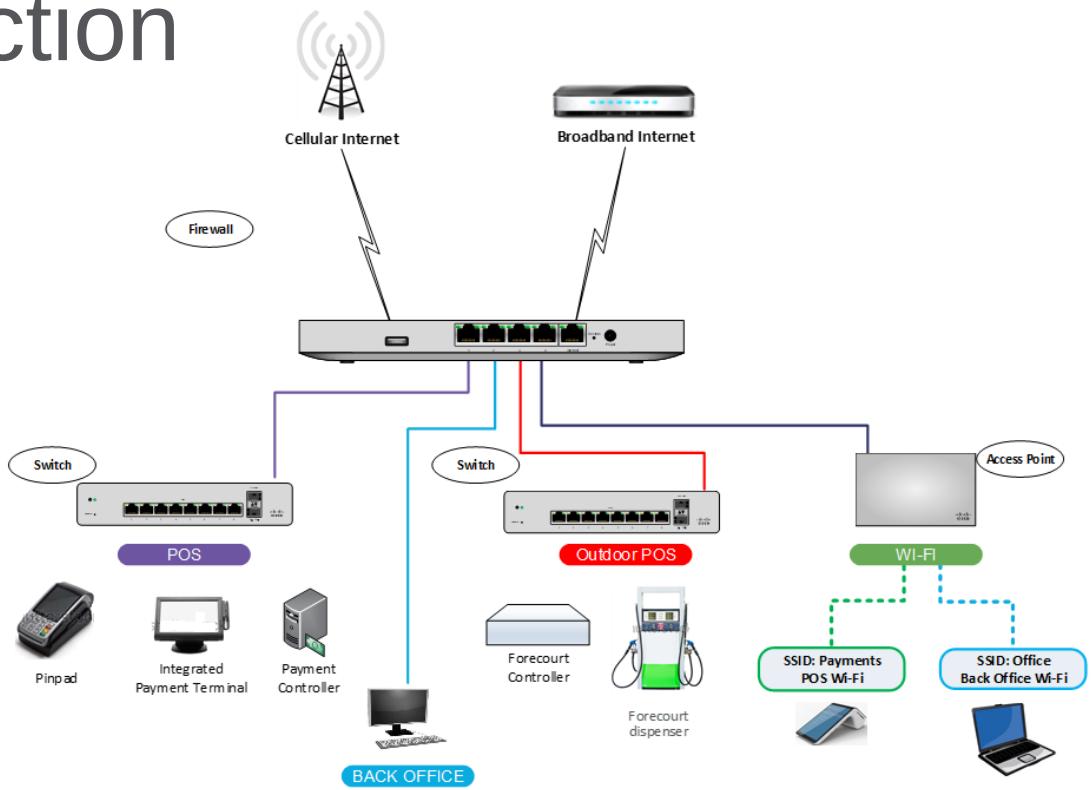
- Managed Detection and Response (MDR) is an all-encompassing cybersecurity service used to detect and respond to cyber-attacks.
- Performed by a 24x7x365 Security Operations Team.
- Backed through intelligence consisting of global threat feeds, behavioral and pattern based threat detection, and analyst driven threat hunting.

How does it work?

- Agent-based collection of hundreds to millions of events every hour.
- Parsing of event data for correlation of threats across multiple sources.
- Alerting of threats followed by human analyst interpretation and review.

Managed Detection

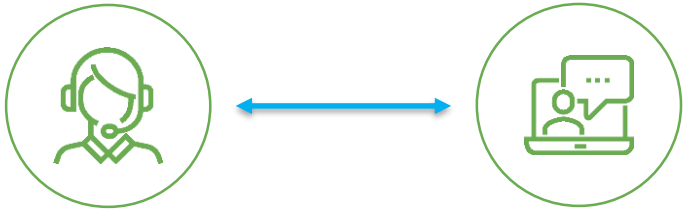
Why is this valuable?



CONEXXUS solve forward

Scenario 1: Remote Access

- **POS Vendor Support connects from remote source to your systems**
  - How do you know it was them?
  - How are you monitoring the activity?
  - How do you separate malicious activity?



CONEXXUS
solve forward

Scenario 1: Remote Access

January 21st 2019, 22:27:09.398 - 09[IKE] initiating IKE_SA Supp-RemoteDesk[85632] to 199.71.10X.XXX

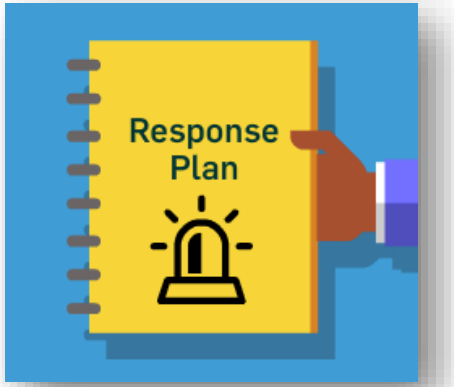
January 21st 2019, 22:27:13.568 - 08[IKE] IKE_SA Supp-RemoteDesk[85632] established between 10.XX.XX.50[35.XXX.XXX.48]...199.71.10X.XXX[199.71.10X.XXX]

January 22nd 2019, 06:17:25.668 - 11[IKE] deleting IKE_SA Supp-RemoteDesk[85632] between 10.XX.XX.50[35.XXX.XXX.48]...199.71.10X.XXX[199.71.10X.XXX]

- Track Remote Access activity based on VPN ID generated at time of initial connection
- Identify source IP of VPN request (199.71.10X.XX)
- Identify connection was successful
- Identify when the connection is terminated
- Correlate this data against EPS/Controller and system logs

Scenario 1: Remote Access

- **Payments Controller attempts remote connection**
  - Detect, Investigate, Respond
  - Quick detection, validation of whether the access occurred
  - Correlate the Who, What, Why, When, Where
  - Establish response plan for action!



CONEXXUS
solve forward

Scenario 1: Remote Access

- EPS/Controller attempts a network inbound/outbound connection

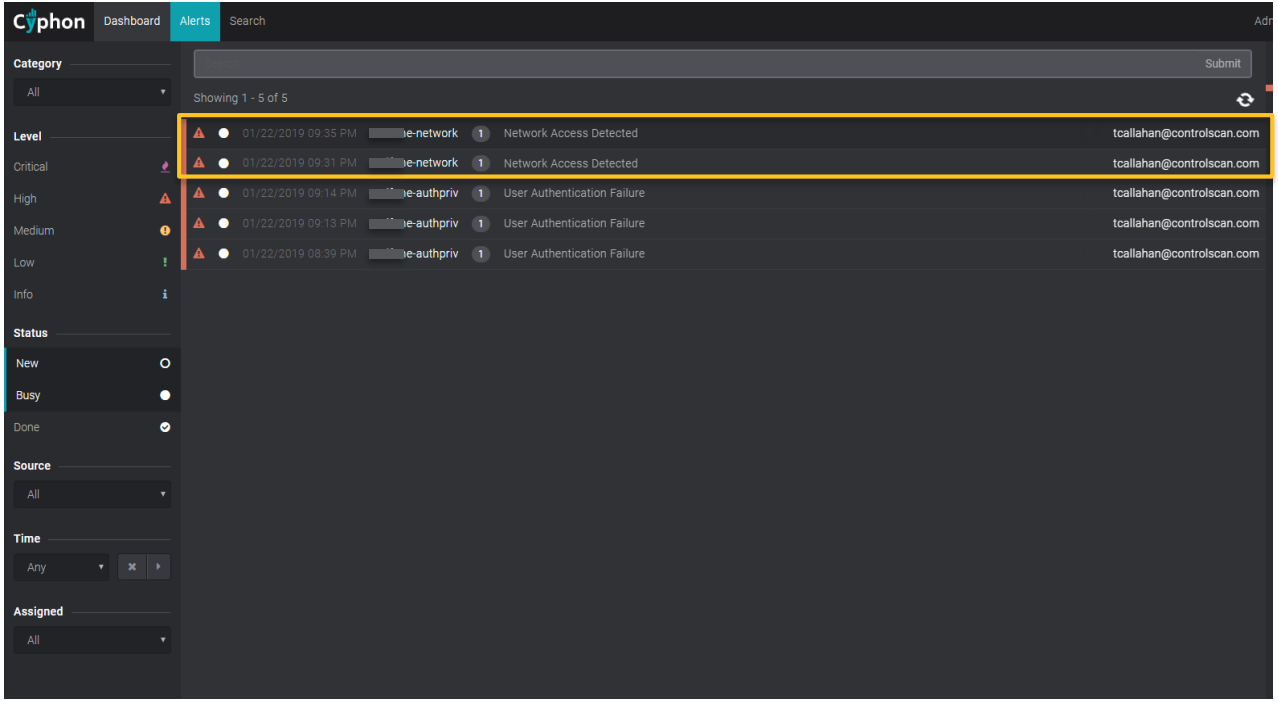
NET CONNECT SEVERITY[LOW]: IN=eth0 OUT=eth0 MAC=16:93:e8:b2:2b:04:16:b9:0b:94:8b:58:08:00 SRC=100.64.4.23 DST=11.1.120.11 LEN=48 TOS=0x00 PREC=0x00 TTL=125 ID=32244 DF PROTO=TCP SPT=59462 DPT=22 WINDOW=8192 RES=0x00 SYN URGP=0

Using this information, we identify:

- Internal classification of Severity, based on existing rulesets
- Source IP Address
- Destination IP Address
- Protocol of the traffic
- Destination Port (22 is SSH)

This then allows us to identify the activity, alert, investigate, and correlate against other datasets. We can use this to determine whether this traffic is expected (logged in user initiated non-malicious traffic), or whether this is unknown or unexpected traffic that could be malicious in nature.

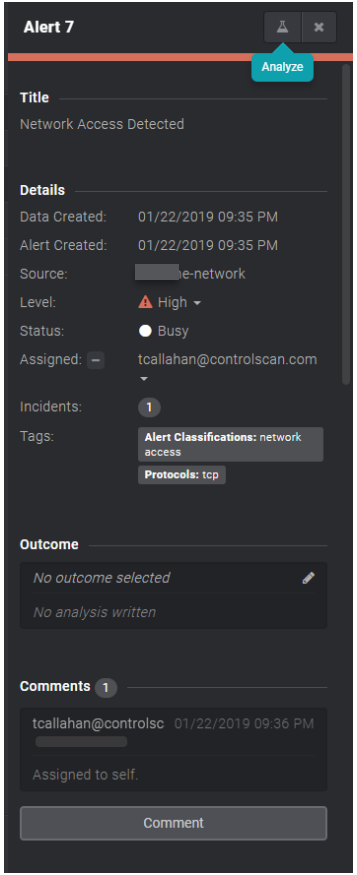
Scenario 1: Remote Access



CONEXXUS
solve forward

Scenario 1: Remote Access

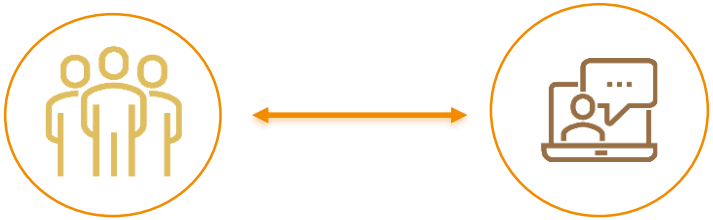

```
▼ Object
  @timestamp: "2019-01-23T02:35:10.753Z"
  AlertTitle: "Network Access Detected"
  dest_ip: "11.1.120.11"
  dest_port: "22"
  ► dst_geoip: Object
  facility_label: "kern"
  host: "gateway"
  logsource: "11.1.5.11"
  message: "[redacted] SEVERITY[LOW]: IN=eth0 OUT=eth0
  MAC=16:93:e8:b2:2b:04:16:b9:0b:94:8b:58:08:00 SRC=8.4.5.8 DST=11.1.120.11 LEN=48
  TOS=0x00 PREC=0x00 TTL=125 ID=32244 DF PROTO=TCP SPT=59462 DPT=22 WINDOW=8192
  RES=0x00 SYN URGP=0"
  port: 44474
  priority: "4"
  program: "kernel"
  relayhost: "11.1.5.11"
  relayip: "11.1.5.11"
  ► severity: Array[2]
  severity_label: "warning"
  source_ip: "8.4.5.8"
  ► src_geoip: Object
  src_port: "59462"
```

CONEXXUS solve forward

Scenario 2: System Access / Authentication

- **Vendor or partner is accessing the system**
  - Detect, Investigate, Respond
  - What actions were taken?
  - Were any changes made?



CONEXXUS
solve forward

Scenario 2: System Access / Authentication

Example 1:
Accepted publickey for centos from 12.190.XX.XX port 54515 ssh2

pam_unix(sshd:session): session opened for user centos by (uid=0)

joeuser : TTY=pts/0 ; PWD=/home/joeuser ; USER=root ; COMMAND=/bin/su

Example 2:
host102 su 1206 - - Successful su for joeuser by root

host102 sudo - - - joeuser : TTY=unknown ; PWD=/home/joeuser ; USER=root ; COMMAND=/usr/local/bin/backupSettings

host102 su 1206 - - pam_unix(su:session): session closed for user joeuser

Scenario 3: System Access / Authentication – FAILURE

- Vendor or partner is attempting access to the system
  - Detect, Investigate, Respond
  - Could be mistyped passwords…. Could be password spray attack
  - Alerting – one or two versus more attempts

Scenario 3: System Access / Authentication – FAILURE

<85>1 2019-01-21T08:41:30.300912-05:00 sourcesystem sshd 6435 - - pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.3X.XX.50 user=root

Here we can identify:

- Date/Time
- Source of login (SSH Daemon)
- Failure, success, etc.
- The remote host or source of the attempt
- The attempted user

Based on this activity, it could just be bad password, mistyped, or other scenario that is not malicious. But we would continuously monitor these types of activities and if they are recurring or hit thresholds (more than 10 in 15 minutes or similar), we would alert and develop the response plan for remediation.

Scenario 3: System Access / Authentication – FAILURE

Data | Related Data | Locations | IP Addresses

[redacted]e-authpriv

AlertTitle
TextField

dest_ip
GenericIPAddressField

dest_port
IntegerField

dst_geoip.city_name
CharField

dst_geoip.continent_code
CharField

dst_geoip.country_code2
CharField

dst_geoip.country_name
CharField

▼ Object

@timestamp: "2019-01-23T01:39:11.623Z"
AlertTitle: "User Authentication Failure"
facility_label: "authpriv"
host: "gateway"
logsource: "[redacted]"
message: "<85>1 2019-01-22T20:39:11.623236-05:00 commander_a sshd 6501 - - pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.32.17.50 user=badguy"
port: 41870
priority: "85"
program: "sshd"
relayhost: "11.1.5.11"
relayip: "11.1.5.11"
severity: "5"
severity_label: "notice"
user: "badguy"

CONEXXUS solve forward

Managed Detection

- Other Logs and Security Data
  - VPN access to system
  - System updates or activities
  - Firewall modifications
  - Etc.

All actionable data, with the right correlation, and the right intelligence behind the screen.

Questions to ask:

How much data do I have?

- Organization with 50 employees:
  - Network equipment (Internet router, firewall, desktops/laptops, POS terminals)
  - Wireless (access points)
  - Devices (IoT, i.e. pump monitoring devices)
- **Average of 750-1,000 logs per second**
- **50 million logs per day (accounting for variance while closed)**
- How are you monitoring that much data?

Questions to ask:

How important is this data?

- Threats appear consistently in these logs:
  - Invalid network traffic
  - Authentication failures (brute force attacks)
  - User access or account modifications
- Threat actors breach one system, and then move laterally into the rest of your network.
- Logs can detect this activity, and notify of a security event.
- **Real-time monitoring identifies this activity in minutes/hours instead of days/months!**

Kill Chain – Anatomy of an Attack

RECONNAISSANCE + INITIAL ATTACK

GOAL

- Harvest information
- Access to network
- Determine target strategy

ACTION

- Social engineering
- Purchase stolen credentials / info on dark web
- Scanning open ports
- Inspecting publicly facing assets
- Searching for vulnerable websites

ESTABLISH FOOTHOLD

GOAL

- Set up comm back to "home"

ACTION

- Cryptomining
- Reverse Shell
- C2 (command and control)
- Persistent backdoor
- Escalate
  - Local Admin
  - Domain Admin
  - Privileged User

DISCOVER

GOAL

- Find new assets
- Identify targeted data

ACTION

- Scan the network
- Responder - NTLM
- Review files available

SPREAD

GOAL

- Spread foothold
- Get keys to the kingdom

ACTION

- SMB enumeration
- Move laterally (credentials)
- Move to escalate
  - Local Admin
  - Domain
  - Admin
  - Privileged User

EXECUTE OBJECTIVES

ACTION

- Remotely carries out intended goal

CONEXXUS solve forward

Managed Detection + Response

What about Response?

- Analysts provide immediate action plans to actively block or prevent malicious activity
- Quarantine host or systems from the network
- Block network traffic through firewall rules and monitoring
- Remediate the threat to get the systems back online quickly, and securely
- Triage with internal and incident response teams to provide larger scale response plans and activities

Questions to ask:

Why does my company or organization need MDR?

- Investments in tools and security products is not enough.
  - Are you watching and taking action on alerts from your security systems?
  - Who is managing your Endpoint Protection software and remediating threats?
- Companies/organizations are constantly under attack.
  - Most are the result of drive by attacks—you are caught in the crossfire of who your Internet or network provider is
  - Others are targeted attacks, designed specifically for your network and employees
- The average detection time for a breach is over 6 months.
  - Can you wait that long to find out malicious actors are in your network and stealing your data?
- Regulators and compliance are getting more strict.
  - Can you afford the cost of a breach or a business outage?

Questions to ask:

What about my existing tools?

- Firewalls and IDS/IPS Devices
  - Yes…100 times yes!
  - First lines of defense and detection
  - Keep them patched, updated, etc.
- Antivirus, AntiMalware, AETP, EDR…
  - All necessary to have… but who is updating the policies?
  - Who is responding and mitigating the alerts?
  - How are you correlating this ensure no lateral movement occurred?
- Others
  - SIEM tools – great in theory, but who is monitoring?
  - Application whitelisting – I'm sure you are tuning this daily/weekly… right?

Managed Detection and Response (MDR)

The Silver Bullet? Far from Reality.

You need a corporate cybersecurity program.

- MDR provides a mechanism to keep eyes on the prize, and to keep the prize in your hands.
- Still need IT Controls, Risk Assessment, DevSecOps
  - System and Application Monitoring and Patching
  - Security Policies including Desktops, Laptops, Mobile Devices, BYOD, Servers, etc.
  - Ongoing Risk Assessment integrated with Operations and Finance Teams
  - DevSecOps – Integration of Development (both IT and non-IT), Security Teams, and Operations
- You need a plan… a documented plan that is reviewed often as a company, not as an individual.

Questions?

- Website: www.conexxus.org
- Email: info@conexxus.org
- LinkedIn Profile: Conexxus.org
- Follow us on Twitter: @Conexxusonline