Eight Keys
to a
Defensible Network Architecture
and
How Zeek Can Help You Get There

Richard Bejtlich and Matt Bromiley

6 November 2018

Speakers

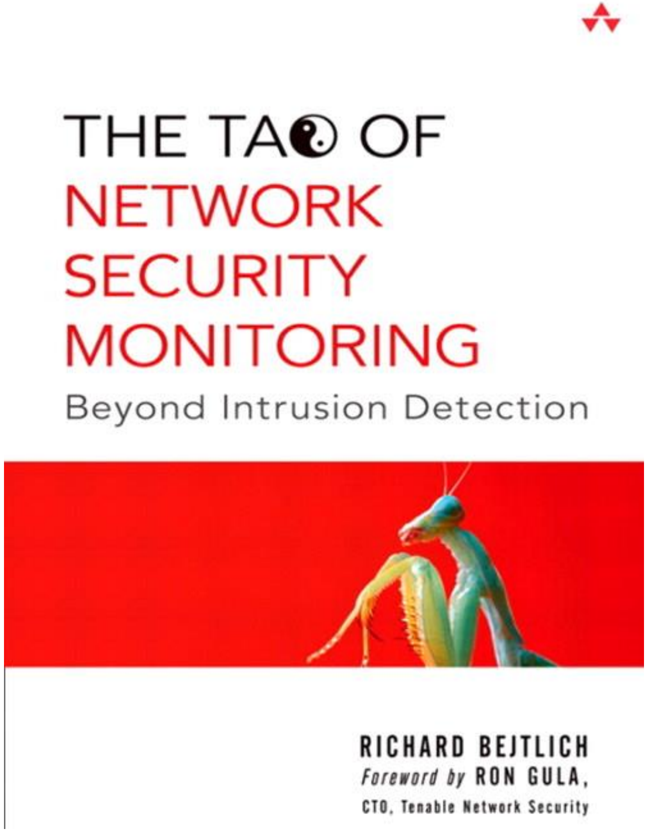
Richard Bejtlich, Corelight

@taosecurity

Matt Bromiley, SANS & Incident Responder

@mbromileydfir

Defensible Network Architecture Intro (2004)



Throughout this book, we will examine intruder actions and the network traffic associated with those activities. Familiarity with these patterns enables defenders to apply their understanding across multiple protection and detection products. Like design patterns in software development, an understanding of intruder activities will bear more fruit than intimate knowledge of one or two exploits sure to become dated in the years to come.

SECURITY PRINCIPLES: DEFENSIBLE NETWORKS

I use the term **defensible networks** to describe enterprises that encourage, rather than frustrate, digital self-defense. Too many organizations lay cables and connect servers without giving a second thought to security consequences. They build infrastructures that any army of defenders could never protect from an enemy. It's as if these organizations used chain-link fences for the roofs of their buildings and wonder why their cleaning staff can't keep the floors dry.

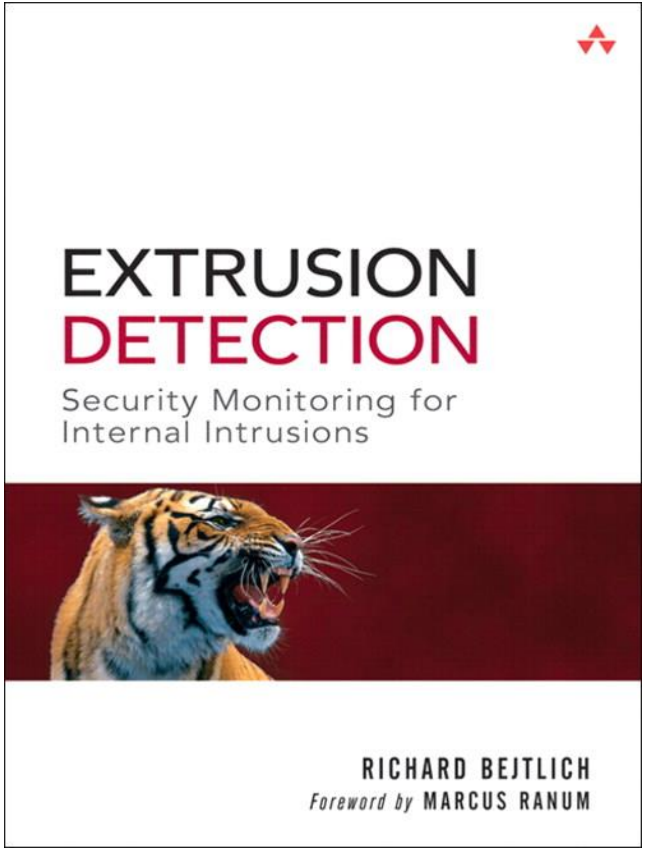
This section describes traits possessed by defensible networks. As you might expect, defensible networks are the easiest to monitor using NSM principles. Many readers will sympathize with my suggestions but complain that their management disagrees. If I'm preaching to the choir, at least you have another hymn in your songbook to show to your management. After the fifth compromise in as many weeks, perhaps your boss will listen to your recommendations!

DEFENSIBLE NETWORKS CAN BE WATCHED

This first principle implies that defensible networks give analysts the opportunity to observe traffic traversing the enterprise's networks. The network was designed with monitoring in mind, whether for security or, more likely, performance and health purposes. These organizations ensure every critical piece of network infrastructure is accessible and offers a way to see some aspects of the traffic passing through it. For example, engineers equip Cisco routers with the appropriate amount of random access memory (RAM) and the necessary version of Internetwork Operating System (IOS) to collect statistics and NetFlow data reflecting the sort of traffic carried by the device. Technicians deploy switches with Switched Port ANalyzer (SPAN) access in mind. If asymmetric routing is deployed at the network edge, engineers use devices capable of making sense of the mismatched traffic patterns. (This is a feature of the new Proventia series of IDS appliances announced by Internet Security Systems, Inc., in late 2003.) If the content of encrypted Web sessions must be analyzed, technicians attach IDSs to SSL accelerators that decrypt and reencrypt traffic on the fly.

A defensible network is an information architecture that is *monitored, controlled, minimized, and current*.

DNA Implementation (2005)



2 Defensible Network Architecture

Far too few networks are built with security in mind. They are generally designed using the day's predominant technology, and they place performance ahead of defense. With Ethernet-based local area networks, for example, we have seen the transition from half-duplex 10 Mbps links, to full-duplex, switched 100 Mbps links. Gigabit Ethernet at 1000 Mbps is being adopted, with sub-$70 eight-port Gigabit switches marketed to home users.

While these new technologies increase the data-carrying capacity of the network, speed has come at the expense of visibility. On a half-duplex 10 Mbps link, each node can see all traffic. Monitoring is simple when one can connect a probe into a classic single-speed hub. With switched, full-duplex networks, other approaches must be taken. (Those approaches are explained in Chapter 4.)

Beyond technological concerns, security analysts must address measurement problems. Issues that can be easily measured receive more attention than those that cannot. Users complain when the "network is slow," not when a stealthy intruder has infiltrated their organization. Therefore, administrators will notice and react to a heavily used pipe before they take action on security matters.[1]

Chapter 1 defined a defensible network as an information architecture that is monitored, controlled, minimized, and current. The order of these principles reflects my belief about their ease of adoption. Relatively speaking, it is easier to monitor than it is to control, easier

1. In some cases, I refer readers to other published resources. For example, I recommend that readers wishing to learn more about firewalls read either one of the several excellent books devoted entirely to the subject or the exceptional Internet Firewall FAQ at http://www.compuwar.net/pubs/fwfaq/.

Extrusion Detection offered implementation guidance using open source tools.

DNA 2.0 (2008)

TaoSecurity

Richard Bejtlich's blog on digital security, strategic thought, and military history.

Thursday, January 10, 2008

Defensible Network Architecture 2.0

Four years ago when I wrote The Tao of Network Security Monitoring I introduced the term **defensible network architecture**. I expanded on the concept in my second book, Extrusion Detection. When I first presented the idea, I said that a defensible network is an information architecture that is monitored, controlled, minimized, and current. In my opinion, a defensible network architecture gives you the best chance to **resist** intrusion, since perfect intrusion prevention is impossible.

I'd like to expand on that idea with Defensible Network Architecture 2.0. I believe these themes would be suitable for a strategic, multi-year program at any organization that commits itself to better security. You may notice the contrast with the Self-Defeating Network and the similarities to my Security Operations Fundamentals. I roughly order the elements in a series from least likely to encounter resistance from stakeholders to most likely to encounter resistance from stakeholders.

A Defensible Network Architecture is an information architecture that is:

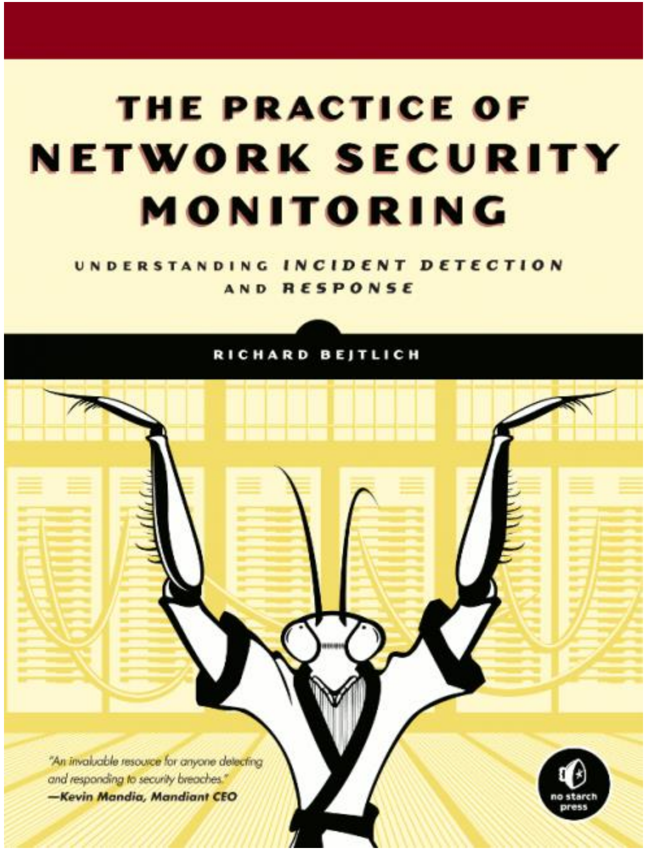
1. **Monitored**. The easiest and cheapest way to begin developing DNA on an existing enterprise is to deploy Network Security Monitoring sensors capturing session data (at an absolute minimum), full content data (if you can get it), and statistical data. If you can access other data sources, like firewall/router/IPS/DNS/proxy/whatever logs, begin working that angle too. Save the tougher data types (those that require reconfiguring assets and buying mammoth databases) until much later. This needs to be a quick win with the data in the hands of a small, centralized group. You should always start by monitoring first, as Bruce Schneier proclaimed so well in 2001.

TaoSecurity Blog expanded DNA with v 2.0:

A defensible network is an information architecture that is monitored, inventoried, controlled, claimed, minimized, assessed, and current.

A comment to the blog by Göran Sandahl suggested adding “*measured*,” which I liked.

DNA 2.1 (2013)



WHAT IS A DEFENSIBLE NETWORK ARCHITECTURE?

Identifying a compromised asset, finding a responsible owner, and delivering an incident report are three of the toughest jobs in security, but they are not the only challenges. I developed a *defensible network architecture* to explain the characteristics of organizations whose network offers the greatest overall security (*http://taosecurity.blogspot.com/2008/01/defensible-network-architecture-20.html*). The list starts with the characteristics a security team should adopt first, and as it continues, the elements become progressively more difficult to implement.

Monitored CIRTs can view all assets at the host, network, and application log levels.
Inventoried CIRTs can access an inventory identifying asset location, purpose, data classification, criticality, owner, and contact method.
Controlled The security team enforces access control at the host, network, and application levels to permit authorized activities and deny everything else.
Claimed The asset owner listed in the inventory exerts active control of the system.
Minimized The assets provide the minimum surface area required to perform their business function; unnecessary services, protocols, and software are disabled.
Assessed The CIRT routinely evaluates the configuration of the assets to determine their security posture.
Current The IT team keeps the assets patch status and configuration up-to-date with the latest standards.
Measured The IT team and CIRT measure their progress against the previous steps.

Organizations that adopt a defensible network architecture are best positioned to resist compromise and to respond effectively to intrusions as they occur.

[The Practice of NSM] published DNA 2.1 in 2013.

DNA 2.1. Monitored

CIRTs can view all assets at the host, network, and application log levels.

DNA 2.1. Inventoried

CIRTs can access an inventory identifying asset location, purpose, data classification, criticality, owner, and contact method.

DNA 2.1. Controlled

The security team enforces access control at the host, network, and application levels to permit authorized activities and deny everything else.

DNA 2.1. Claimed

The asset owner listed in the inventory exerts active control of the system.

DNA 2.1. Minimized

The assets provide the minimum surface area required to perform their business function; unnecessary services, protocols, and software are disabled.

DNA 2.1. Assessed

The CIRT routinely evaluates the configuration of the assets to determine their security posture.

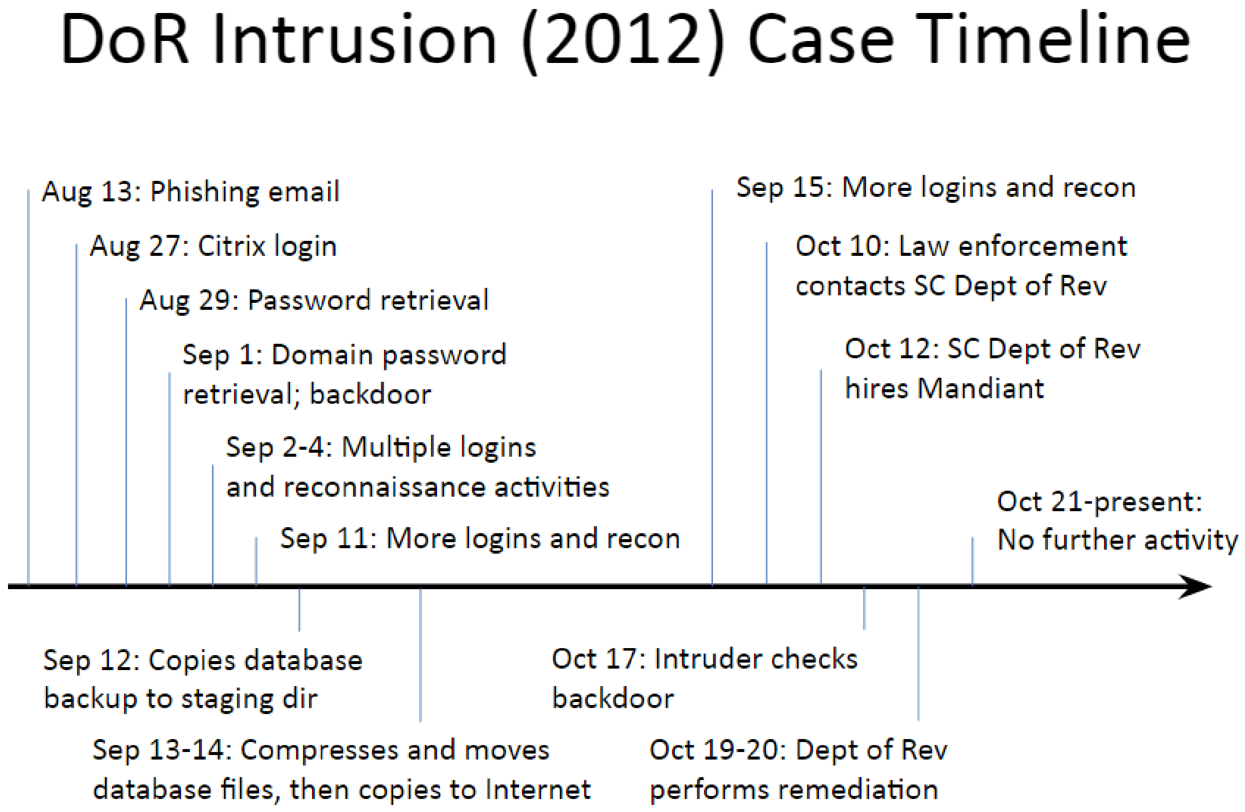
DNA 2.1. Current

The IT team keeps the assets patch status and configuration up-to-date with the latest standards.

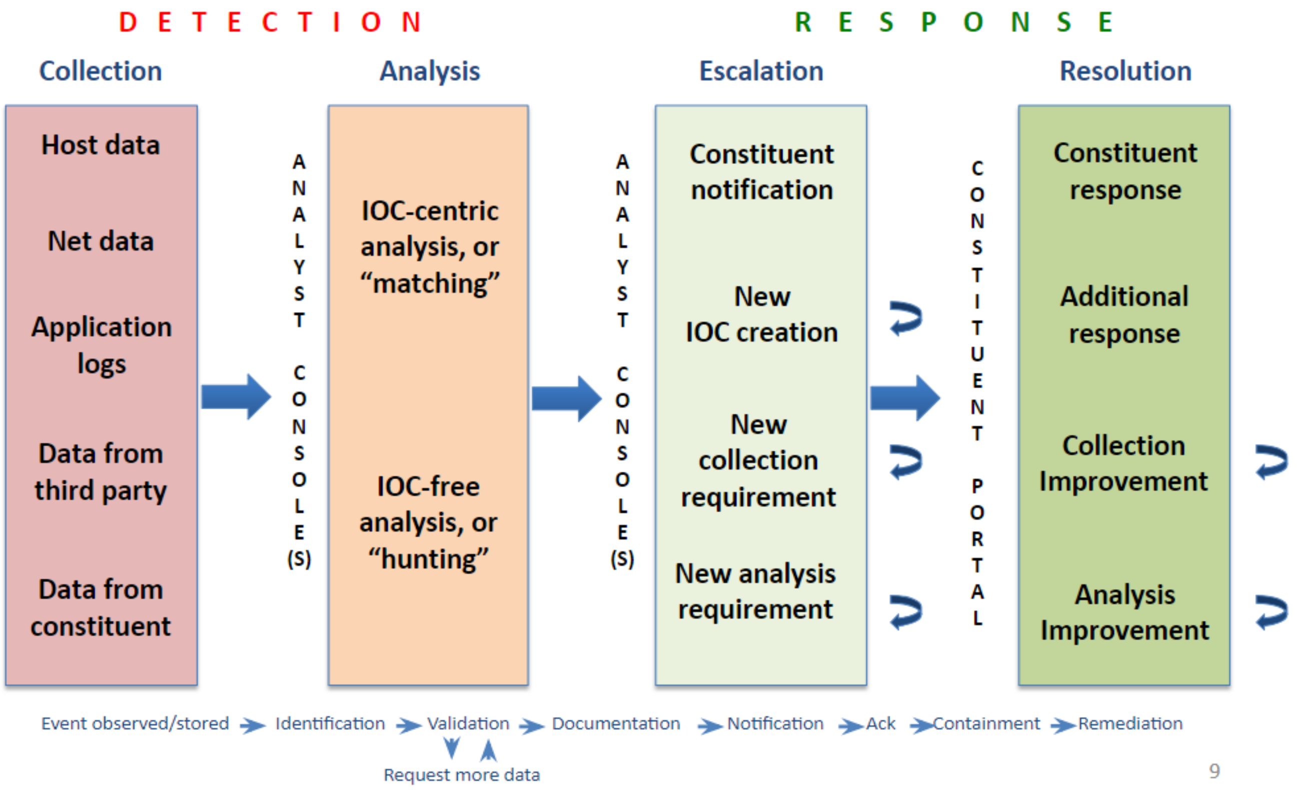
DNA 2.1. Measured

The IT team and CIRT measure their progress against the previous steps.

DNA 2.1. Why?


DoR Intrusion (2012) Case Timeline
Aug 13: Phishing email
Aug 27: Citrix login
Aug 29: Password retrieval
Sep 1: Domain password retrieval; backdoor
Sep 2-4: Multiple logins and reconnaissance activities
Sep 11: More logins and recon
Sep 12: Copies database backup to staging dir
Sep 13-14: Compresses and moves database files, then copies to Internet
Sep 15: More logins and recon
Oct 10: Law enforcement contacts SC Dept of Rev
Oct 12: SC Dept of Rev hires Mandiant
Oct 17: Intruder checks backdoor
Oct 19-20: Dept of Rev performs remediation
Oct 21-present: No further activity

DNA 2.1. Relationship to NSM



DNA 2.1. Monitored with Zeek

CIRTs can view all assets at the host, network, and application log levels.

conn.log

1541195769.387339	Cx6D4h3VZUct7k0Qn7	172.16.8.195	49372	31.13.93.35	80	tcp	http	0.224698	
1541195745.926661	Cd5uD63lbCZOughoAb	172.16.8.195	49359	83.166.138.8	443	tcp	ssl	3.926521	
1541195815.092111	CLhVk01AnTOxnx0jb4	172.16.8.195	49409	62.2.99.251	80	tcp	http	0.672406	
1541195834.312922	CKTjSi4GVpgIyDYo26	172.16.8.195	49426	149.126.4.83	80	tcp	http	0.566245	
1541195818.884242	C9Iwln23lnq9hPWpo5	172.16.8.195	49413	62.2.99.251	443	tcp	ssl	1.532328	
1541195759.074617	CcRkgw21a81uLqK643	172.16.8.195	49364	193.200.231.5	80	tcp	http	0.462417	
1541195713.360640	CkyBSj4pOtPvysUA68	172.16.8.195	49342	89.107.184.10	80	tcp	http	65.689622	
1541195735.605880	CWudWA7fLWxL65lR6	172.16.8.195	49356	34.246.51.179	80	tcp	http	60.087822	
1541195815.766748	C2wgbm1yNr062jrxU3	172.16.8.195	49410	62.2.99.251	443	tcp	ssl	1.130583	
1541195762.015389	C2ibnv4ukh6Zaslc3d	172.16.8.195	49367	194.51.187.22	80	tcp	http	0.400956	
1541195787.412528	Caz5BR3OvdYza0plt	172.16.8.195	49384	107.154.110.25	80	tcp	http	0.522343	
1541195807.613279	Cf5fnF381tPTdELYzc	172.16.8.195	49399	145.239.37.26	80	tcp	http	2.334841	
1541195838.425998	CwTvWv2FiFV1msef5a	172.16.8.195	49432	149.202.81.123	443	tcp	ssl	0.684731	
1541195714.104829	CE8XM5WXSLTyAILR5	172.16.8.195	49343	89.107.184.10	443	tcp	ssl	66.373964	
1541195810.627697	Cpl8GE4M0riqqwj5J4	172.16.8.8	138	172.16.8.255	138	udp	-	-	-

DNA 2.1. Monitored with Zeek

CIRTs can view all assets at the host, network, and application log levels.

software.log

```
10.1.75.167      -      HTTP::BROWSER    Microsoft NCSI  -       -       -       -       -       Microsoft NCSI
10.1.75.167      -      HTTP::BROWSER    MSIE    11      0       -       -       -       Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
190.107.177.240  80     HTTP::SERVER     Apache  -       -       -       -       -       Apache
190.107.177.240  80     HTTP::APPSERVER  PHP     7       0       31      -       -       PHP/7.0.31
23.229.231.33    80     HTTP::SERVER     Apache  -       -       -       -       -       Apache
23.229.231.33    80     HTTP::APPSERVER  PHP     5       6       36      -       -       PHP/5.6.36
87.66.13.80      80     HTTP::SERVER     nginx   -       -       -       -       -       nginx
10.1.75.167      -      HTTP::BROWSER    Chrome  60      0       3112    113     -       Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
54.243.123.39    80     HTTP::SERVER     Cowboy  -       -       -       -       -       Cowboy
192.161.54.60    80     HTTP::SERVER     nginx   1       6       2       -       -       nginx/1.6.2
10.1.75.167      -      HTTP::BROWSER    WinHTTP loader  1       0       -       -       -       WinHTTP loader/1.0
10.1.75.4        -      HTTP::BROWSER    WinHTTP sender  1       0       -       -       -       WinHTTP sender/1.0
200.29.24.36     8082   HTTP::SERVER     Cowboy  -       -       -       -       -       Cowboy
10.1.75.4        -      HTTP::BROWSER    WinHTTP loader  1       0       -       -       -       WinHTTP loader/1.0
72.149.206.152   80     HTTP::SERVER     nginx   -       -       -       -       -       nginx
```

DNA 2.1. Inventoried with Zeek

CIRTs can access an inventory identifying asset location, purpose, data classification, criticality, owner, and contact method.

dhcp.log

```
1541195390.021352  Cm6XiT2QMUQ9FSDyKa   255.255.255.255 68   172.16.8.8   67   00:08:02:1c:47:ae   172.16.8.195
1541195393.402442  C0PF7s30vQxd7mahi6   172.16.8.195    68   172.16.8.8   67   00:08:02:1c:47:ae   172.16.8.195
1541195453.811267  CZMOMcY9CKGNdspLj    172.16.8.195    68   172.16.8.8   67   00:08:02:1c:47:ae   172.16.8.195
1541195549.313016  CZMOnyVsLpqdwBaf8    172.16.8.195    68   172.16.8.8   67   00:08:02:1c:47:ae   172.16.8.195
```

software.log

```
10.1.75.167      -     HTTP::BROWSER   Microsoft NCSI  -    -     -    -    -   Microsoft NCSI
10.1.75.167      -     HTTP::BROWSER   MSIE     11     0    -     -    -    Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
190.107.177.240  80    HTTP::SERVER    Apache   -      -    -     -    -    Apache
190.107.177.240  80    HTTP::APPSERVER PHP      7      0    31    -    -    PHP/7.0.31
23.229.231.33    80    HTTP::SERVER    Apache   -      -    -     -    -    Apache
23.229.231.33    80    HTTP::APPSERVER PHP      5      6    36    -    -    PHP/5.6.36
87.66.13.80      80    HTTP::SERVER    nginx    -      -    -     -    -    nginx
10.1.75.167      -     HTTP::BROWSER   Chrome   60     0    3112  113  -    Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
54.243.123.39    80    HTTP::SERVER    Cowboy   -      -    -     -    -    Cowboy
192.161.54.60    80    HTTP::SERVER    nginx    1      6    2     -    -    nginx/1.6.2
10.1.75.167      -     HTTP::BROWSER   WinHTTP loader  1    0     -    -    -   WinHTTP loader/1.0
10.1.75.4        -     HTTP::BROWSER   WinHTTP sender  1    0     -    -    -   WinHTTP sender/1.0
200.29.24.36     8082  HTTP::SERVER    Cowboy   -      -    -     -    -    Cowboy
10.1.75.4        -     HTTP::BROWSER   WinHTTP loader  1    0     -    -    -   WinHTTP loader/1.0
72.149.206.152   80    HTTP::SERVER    nginx    -      -    -     -    -    nginx
```

DNA 2.1. Controlled with Zeek?

The security team enforces access control at the host, network, and application levels to permit authorized activities and deny everything else.

Exploit-specific blocking

```
Apr  9 01:58:17 acld: NETS status=success cmd=nullzero id=wired device=
ip=107.3.148.68 ats=1397033897.178419 cts=1397033897.178482
cmt={bro@} no=Heartbleed::SSL_Heartbeat_Attack msg=An TLS heartbleed attack was
detected! Record length 3, payload length 16384
```

Credit: https://www.bro.org/brocon2014/brocon2014_sharma_active_defense.pdf

DNA 2.1. Controlled with Zeek?

The security team enforces access control at the host, network, and application levels to permit authorized activities and deny everything else.

On-the-fly Connection ACLs

```
Aug 17 02:43:27  NETS status=success cmd=nullzero id=wired device=XXXX
ip=1.50.224.173 ats=1408268607.940360 cts=1408268607.940412 cmt={bro@}"
 no=OldScan::AddressScan msg=1.50.224.173 has scanned      hosts 23/tcp \
'
```

Credit: https://www.bro.org/brocon2014/brocon2014_sharma_active_defense.pdf

DNA 2.1. Claimed with Zeek?

The asset owner listed in the inventory exerts active control of the system.

dhcp.log

1541195390.021352	Cm6XiT2QMUQ9FSDyKa	255.255.255.255	68	172.16.8.8	67	00:08:02:1c:47:ae	172.16.8.195
1541195393.402442	C0PF7s30vQxd7mahi6	172.16.8.195	68	172.16.8.8	67	00:08:02:1c:47:ae	172.16.8.195
1541195453.811267	CZMOMcY9CKGNdspLj	172.16.8.195	68	172.16.8.8	67	00:08:02:1c:47:ae	172.16.8.195
1541195549.313016	CZMOnyVsLpqdwBaf8	172.16.8.195	68	172.16.8.8	67	00:08:02:1c:47:ae	172.16.8.195

kerberos.log

172.16.8.195	49160	172.16.8.8	88	AS	humble-dan-pc$/GONEAWRY.NET	krbtgt/GONEAWRY.NET	F	KDC_ERR_PREAUTH_REQUIRED			
172.16.8.195	49161	172.16.8.8	88	AS	humble-dan-pc$/goneawry.net	krbtgt/goneawry.net	F	KDC_ERR_PREAUTH_REQUIRED			
172.16.8.195	49162	172.16.8.8	88	AS	humble-dan-pc$/GONEAWRY.NET	krbtgt/GONEAWRY.NET	T	-	-	213642288	
172.16.8.195	49163	172.16.8.8	88	TGS	HUMBLE-DAN-PC$/GONEAWRY.NET	LDAP/Goneawry-DC.goneawry.net/goneawry.net	T	-			
172.16.8.195	49165	172.16.8.8	88	AS	humble-dan-pc$/goneawry.net	krbtgt/GONEAWRY.NET	T	-	-	213642288	
172.16.8.195	49166	172.16.8.8	88	TGS	HUMBLE-DAN-PC$/GONEAWRY.NET	cifs/goneawry-dc.goneawry.net	T	-	-	21	
172.16.8.195	49167	172.16.8.8	88	TGS	HUMBLE-DAN-PC$/GONEAWRY.NET	ldap/goneawry-dc.goneawry.net	T	-	-	21	
172.16.8.195	49168	172.16.8.8	88	TGS	HUMBLE-DAN-PC$/GONEAWRY.NET	krbtgt/GONEAWRY.NET	T	-	-	213642288	
172.16.8.195	49171	172.16.8.8	88	TGS	HUMBLE-DAN-PC$/GONEAWRY.NET	ldap/Goneawry-DC.goneawry.net/goneawry.net	T	-			

DNA 2.1. Minimized with Zeek

The assets provide the minimum surface area required to perform their business function; unnecessary services, protocols, and software are disabled.

software.log

1538420062.545530	10.1.75.167	-	HTTP::BROWSER	Microsoft NCSI		-	-	-
1538420133.059265	10.1.75.167	-	HTTP::BROWSER	MSIE	11	0	-	-
1538420133.516514	190.107.177.240	80	HTTP::SERVER	Apache	-	-	-	-
1538420133.516514	190.107.177.240	80	HTTP::APPSERVER	PHP	7	0	31	-
1538420164.048636	23.229.231.33	80	HTTP::SERVER	Apache	-	-	-	-
1538420164.335194	23.229.231.33	80	HTTP::APPSERVER	PHP	5	6	36	-
1538420188.784344	87.66.13.80	80	HTTP::SERVER	nginx	-	-	-	-
1538420268.269950	10.1.75.167	-	HTTP::BROWSER	Chrome	60	0	3112	113
1538420268.481641	54.243.123.39	80	HTTP::SERVER	Cowboy	-	-	-	-
1538420442.319115	192.161.54.60	80	HTTP::SERVER	nginx	1	6	2	-
1538420467.571861	10.1.75.167	-	HTTP::BROWSER	WinHTTP loader		1	0	-
1538420869.452395	10.1.75.4	-	HTTP::BROWSER	WinHTTP sender		1	0	-
1538420869.452395	200.29.24.36	8082	HTTP::SERVER	Cowboy	-	-	-	-
1538420869.848287	10.1.75.4	-	HTTP::BROWSER	WinHTTP loader		1	0	-
1538421162.607214	72.149.206.152	80	HTTP::SERVER	nginx	-	-	-	-

DNA 2.1. Minimized with Zeek

The assets provide the minimum surface area required to perform their business function; unnecessary services, protocols, and software are disabled.

weird.log

10.1.75.167	49168	10.1.75.4	49158	unknown_dce_rpc_auth_type_68		-
10.1.75.167	57645	10.1.75.4	53	DNS_RR_length_mismatch	-	F
10.1.75.167	62032	10.1.75.4	53	DNS_RR_unknown_type	249	F
10.1.75.167	63452	10.1.75.4	53	DNS_RR_length_mismatch	-	F
10.1.75.167	56407	224.0.0.252	5355	dns_unmatched_msg	-	F
10.1.75.167	51587	224.0.0.252	5355	dns_unmatched_msg	-	F
10.1.75.167	62111	224.0.0.252	5355	dns_unmatched_msg	-	F
10.1.75.167	56674	224.0.0.252	5355	dns_unmatched_msg	-	F
10.1.75.167	137	10.1.75.255	137	dns_unmatched_msg	-	F
10.1.75.167	49164	10.1.75.4	49155	unknown_dce_rpc_auth_type_68		-
10.1.75.167	62052	10.1.75.4	49155	unknown_dce_rpc_auth_type_68		-
10.1.75.167	137	10.1.75.4	137	dns_unmatched_reply	-	F
10.1.75.167	137	10.1.75.4	137	dns_unmatched_msg	-	F
10.1.75.167	62071	10.1.75.4	49158	unknown_dce_rpc_auth_type_68		-
10.1.75.4	137	10.1.75.255	137	dns_unmatched_msg	-	F
10.1.75.4	63721	224.0.0.252	5355	dns_unmatched_msg	-	F
10.1.75.167	137	10.1.75.4	137	dns_unmatched_reply	-	F
10.1.75.167	137	10.1.75.255	137	dns_unmatched_msg	-	F
10.1.75.167	137	10.1.75.4	137	dns_unmatched_msg	-	F
10.1.75.4	137	10.1.75.255	137	dns_unmatched_msg	-	F
10.1.75.4	53486	224.0.0.252	5355	dns_unmatched_msg	-	F
10.1.75.4	137	10.1.75.255	137	dns_unmatched_msg	-	F

DNA 2.1. Assessed with Zeek

The CIRT routinely evaluates the configuration of the assets to determine their security posture.

software.log

```
1538420062.545530   10.1.75.167     -     HTTP::BROWSER   Microsoft NCSI  -       -       -
1538420133.059265   10.1.75.167     -     HTTP::BROWSER   MSIE    11      0       -       -
1538420133.516514   190.107.177.240 80    HTTP::SERVER    Apache  -       -       -       -
1538420133.516514   190.107.177.240 80    HTTP::APPSERVER PHP     7       0       31      -
1538420164.048636   23.229.231.33   80    HTTP::SERVER    Apache  -       -       -       -
1538420164.335194   23.229.231.33   80    HTTP::APPSERVER PHP     5       6       36      -
1538420188.784344   87.66.13.80     80    HTTP::SERVER    nginx   -       -       -       -
1538420268.269950   10.1.75.167     -     HTTP::BROWSER   Chrome  60      0       3112    113
1538420268.481641   54.243.123.39   80    HTTP::SERVER    Cowboy  -       -       -       -
1538420442.319115   192.161.54.60   80    HTTP::SERVER    nginx   1       6       2       -
1538420467.571861   10.1.75.167     -     HTTP::BROWSER   WinHTTP loader  1       0       -
1538420869.452395   10.1.75.4       -     HTTP::BROWSER   WinHTTP sender  1       0       -
1538420869.452395   200.29.24.36    8082  HTTP::SERVER    Cowboy  -       -       -       -
1538420869.848287   10.1.75.4       -     HTTP::BROWSER   WinHTTP loader  1       0       -
1538421162.607214   72.149.206.152  80    HTTP::SERVER    nginx   -       -       -       -
```

DNA 2.1. Current with Zeek

The IT team keeps the assets patch status and configuration up-to-date with the latest standards.

software.log

```
10.1.75.167     -       HTTP::BROWSER    Microsoft NCSI  -       -       -       -       -       Microsoft NCSI
10.1.75.167     -       HTTP::BROWSER    MSIE    11      0       -       -       -       Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
190.107.177.240 80      HTTP::SERVER     Apache  -       -       -       -       -       Apache
190.107.177.240 80      HTTP::APPSERVER  PHP     7       0       31      -       -       PHP/7.0.31
23.229.231.33   80      HTTP::SERVER     Apache  -       -       -       -       -       Apache
23.229.231.33   80      HTTP::APPSERVER  PHP     5       6       36      -       -       PHP/5.6.36
87.66.13.80     80      HTTP::SERVER     nginx   -       -       -       -       -       nginx
10.1.75.167     -       HTTP::BROWSER    Chrome  60      0       3112    113     -       Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
54.243.123.39   80      HTTP::SERVER     Cowboy  -       -       -       -       -       Cowboy
192.161.54.60   80      HTTP::SERVER     nginx   1       6       2       -       -       nginx/1.6.2
10.1.75.167     -       HTTP::BROWSER    WinHTTP loader  1       0       -       -       -       WinHTTP loader/1.0
10.1.75.4       -       HTTP::BROWSER    WinHTTP sender  1       0       -       -       -       WinHTTP sender/1.0
200.29.24.36    8082    HTTP::SERVER     Cowboy  -       -       -       -       -       Cowboy
10.1.75.4       -       HTTP::BROWSER    WinHTTP loader  1       0       -       -       -       WinHTTP loader/1.0
72.149.206.152  80      HTTP::SERVER     nginx   -       -       -       -       -       nginx
```

DNA 2.1. Measured with Zeek

The IT team and CIRT measure their progress against the previous steps.

This one is dependent on your team.
Keep metrics, measure team visibility, and effectiveness.

Q&A

Please use **GoTo**Webinar’s Questions tool to submit questions to our panel.

Send to “Organizers” and tell us if it’s for a specific panelist.