

SANS PROTECTS SERIES

# SANS Protects: The Network

Author: **Matt Bromiley**

Presentation Date: **August 31st, 2022**

Analyst Program 

## OVERVIEW

SANS Protects is a series of papers focused on the most prevalent threats to specific, critical components of your environment as well as actions you can take to mitigate those threats and thwart threat actors. In this paper, we look at threats specific to enterprise networks. Networks are essential to any business environment, connecting every single device and allowing communications to occur. However, networks also act as a conduit that adversaries can use to quickly move through an environment, deploying attacks in record times.

## MEET THE AUTHOR



**Matt Bromiley**  
SANS Certified Instructor

Matt Bromiley is a principal incident response consultant at a top digital forensics and incident response (DFIR) firm. In the DFIR firm Matt assists clients with incident response, digital forensics, and litigation support. He also serves as a GIAC Advisory Board member, a subject-matter expert for the SANS Security Awareness, and a technical writer for the SANS Analyst Program. Matt brings his passion for digital forensics to the classroom as a SANS Instructor for FOR508: Advanced Incident Response, Threat Hunting and Digital Forensics, and FOR572: Advanced Network Forensics, where he focuses on providing students with implementable tools and concepts.

In this SANS Protects paper, we examine current, prevalent network threats and how adversaries use them to take advantage of, and maintain footholds in, victim environments.

This paper also includes an actionable checklist of essential mitigation tips and tricks that organizations can implement to strengthen their security posture.

Some of the threats we investigate include:

- The ease of lateral movement in unsegmented networks
- Unsecured or weakly configured remote access tools
- How adversaries hide their network traffic and manage to steal data
- Abuse of networks protocols, such as DNS, to hide among often uninspected traffic

## SPONSOR

- Sponsors of this highly sought out report can position themselves as a trusted solution provider for the network
- Cobrand the whitepaper and webcast.
- Collaborate with SANS' best cybersecurity experts who are at the forefront of the ever-changing war on cybersecurity.

View next page for sponsorship packages.

# SANS PROTECTS: THE NETWORK

Multi-sponsored Report Sponsorship	GOLD	PLATINUM
<b>Paper</b>		
Branded whitepaper PDF	✓	✓
<b>Report Analysis &amp; Discussion (90-minute virtual presentation)</b>		
Branding on the report presentation registration page	✓	✓
5-minute introduction on presentation		✓
Included in 20–30 minute panel discussion with the report author(s) and platinum sponsors		✓
MP4 Recording of Session		✓
Opt-in Lead Guarantee	300	300

## LEAD SUBMISSION AND REPORT PROMOTIONS

### Lead Submission

The initial installment of leads will be provided within two business days of the live presentation. Additional leads will be provided on a regular basis for the first three months following the presentation. After three months, leads will be provided as requested.

### Promotions

**Presentation:** The presentation will be promoted to the SANS community 7-8 weeks prior to the date.

**Whitepaper:** The whitepaper will be available in the SANS Reading Room on the same day as the presentation and will be promoted to the SANS community.

[Contact your SANS representative](#) today to learn more about sponsoring this SANS report.