# Kinerja Tim Merah untuk Peningkatan Keamanan Komputer

Artikel dalam Prosiding Pertemuan Tahunan Masyarakat Faktor Manusia dan Ergonomi · September 2004

DOI: 10.1177/154193120404801410



**3 penulis,** termasuk:

Sara Kraemer
Universitas Wisconsin–Madison
**24** PUBLIKASI 496 KUTIPAN
LIHAT PROFIL

Pascale Carayon
Universitas Wisconsin–Madison
**428** PUBLIKASI 16.756 KUTIPAN
LIHAT PROFIL

# KINERJA TIM MERAH UNTUK MENINGKATKAN KEAMANAN KOMPUTER

Sara Kraemer+, Pascale Carayon+ dan Ruth Duggan*
+Departemen Teknik Industri Pusat
Peningkatan Kualitas dan Produktivitas Universitas
Wisconsin-Madison 610 Walnut Street
575 WARF Madison, WI 53726
Telp: 1-608- 263-2520
Faks: 1-608-263 -1425
Email:
sbkraeme@wisc.edu / carayon@engr.wisc.edu

* PO Box Laboratorium Nasional
Sandia, 5800, MS-1375
Albuquerque, NM 87185-1375 Telp:
1-505-844-9320 Faks:
1-505-284-9043 Email:
rduggan@sandia.gov

**ABSTRAK**

Penelitian ini mencoba untuk mengembangkan pemahaman faktor manusia tentang strategi penilaian tim merah dalam keamanan komputer dan informasi. Tim merah adalah bentuk penilaian tingkat lanjut yang dapat digunakan untuk mengidentifikasi kelemahan dalam berbagai sistem keamanan. Tujuan dari penelitian ini adalah untuk mengidentifikasi dan mendefinisikan berbagai dimensi efektivitas tim merah dengan tujuan untuk meningkatkan kinerja tim merah. Studi terhadap tim merah dilakukan bekerja sama dengan Tim Merah Jaminan Desain Informasi Laboratorium Nasional Sandia (IDART). Desain penelitiannya meliputi wawancara individu semi terstruktur dan kelompok fokus dengan anggota tim merah serta observasi praktik tim merah. Analisis menghasilkan berbagai dimensi efektivitas tim merah dari sudut pandang pelanggan, manajemen, individu, dan anggota tim.

## PENDAHULUAN DAN LATAR BELAKANG

### Tim merah dalam keamanan komputer dan informasi

Musuh sistem komputer dan informasi dapat dan akan merencanakan dan melaksanakan kampanye serangan strategis terhadap Amerika Serikat (Tinnel, Saydjari, & Farrel, 2002). Departemen Pertahanan telah menyadari bahwa tim merah telah lama menjadi alat yang berharga, meskipun kurang dimanfaatkan, untuk memperdalam pemahaman tentang musuh-musuh yang dihadapi Amerika Serikat dalam perang melawan terorisme (Defense Science Board Task Force, 2003). Secara khusus, kerja sama merah sangat berharga dalam memahami kemampuan musuh dan potensi respons terhadap inisiatif Amerika Serikat (Defense Science Board Task Force, 2003).
Untuk memperluas dan meningkatkan basis pengalaman para pembela sistem, pemahaman yang dikembangkan tentang strategi dan taktik yang digunakan oleh tim merah sangat penting untuk menangkal serangan terhadap komputer dan sistem informasi.

Tim merah mengungkap kelemahan sistem keamanan komputer dan informasi. Penggunaan tim merah (Schudel & Wood, 2000a) dan apa yang disebut “peretasan etis” (lihat, misalnya, Palmer, 2001) merupakan mekanisme penting untuk mendeteksi sistem kerentanan dan karenanya meningkatkan keamanan, karena memungkinkan pembela sistem untuk memahami kelemahan sistem dari sudut pandang musuh. Meskipun 'penegakan keamanan harian' mungkin berhasil untuk sementara waktu, serangan tim merah dan koreksi terhadap cacat yang mereka ungkapkan diperlukan untuk sistem keamanan komputer dan informasi organisasi (Computer Science and Telecommunications Board-National Research Council, 2002). Tulisan ini secara khusus mengkaji Tim Merah Jaminan Desain Informasi Laboratorium Nasional Sandia (IDART). Tujuan dari penelitian ini adalah untuk mengidentifikasi ukuran kinerja tim merah dengan tujuan meningkatkan kinerja tim merah.

Pengetahuan yang diperoleh tim merah sangat bermanfaat ketika sistem target masih dalam pengembangan dan desainer dapat segera melakukan perbaikan (Wood & Duggan, 1999).
Pendekatan tim merah didasarkan pada premis bahwa seorang analis yang mencoba memodelkan musuh dapat menemukan kerentanan sistemik dalam komputer dan sistem informasi yang jika tidak, tidak akan terdeteksi. Mereka mencari peluang untuk menggabungkan kerentanan sistem, organisasi, dan arsitektur agar dapat melakukan serangan yang berhasil. Tim merah Sandia telah mengembangkan metodologi penilaian formal

(Kayu & Duggan, 1999). Metode ini mencakup pembangunan tim, penilaian dan penyerangan sistem, dan pelaporan kepada pelanggan. Bagian penting dari proyek tim merah adalah penilaian sistem. Hal ini mencakup pengumpulan informasi sumber, mendeskripsikan sistem, menciptakan tujuan obyektif, mengidentifikasi faktor penentu keberhasilan, merumuskan fungsional, spasial, temporal, siklus hidup sistem, dan pandangan berbasis konsekuensi dari sistem, mengidentifikasi kandidat kerentanan terhadap serangan, dan merumuskan rencana serangan. Sasaran musuh tertentu yang menghasilkan konsekuensi negatif disebut "bendera". Tim merah telah "merebut bendera" ketika mereka berhasil mencapai tujuan tersebut. Pelanggan tim merah Sandia berasal dari sektor swasta, mulai dari perbankan dan keuangan, teknologi informasi, manufaktur dan e-commerce, serta sektor publik, termasuk Departemen Pertahanan, Energi, Dalam Negeri, Keamanan Dalam Negeri, dan Negara.

Perlunya pemahaman yang lebih komprehensif tentang tim merah. Tidak hanya permintaan yang sangat tinggi terhadap penilaian tim merah, hanya sedikit penelitian yang dilakukan untuk memahami efektivitas penilaian tim merah. Hal ini disebabkan kurangnya ketersediaan, aksesibilitas, dan pendanaan untuk analisis kinerja tim. Tim lebih mungkin berhasil dan efisien ketika mereka mahir dalam mencatat dan mengarsipkan informasi dan berfungsi dalam proses yang sistematis (Lynn & Reilly, 2000), dan seringkali pengetahuan yang diperoleh tim merah hanya dicatat dalam laporan rahasia spesifik proyek atau dibiarkan. untuk kognisi orang-orang dari tim resmi merah. Beberapa penelitian telah dilakukan untuk memahami kinerja tim merah (Carayon, Duggan, & Kraemer, 2003), namun informasi yang lebih banyak dan lebih baik diperlukan untuk mendefinisikan dan mengukur kinerja tim merah agar memiliki dampak yang lebih berarti pada mitigasi kerentanan, keamanan. pelanggaran, dan serangan. Secara khusus, ukuran kinerja tim merah yang diformalkan diperlukan untuk memantau kinerja dari waktu ke waktu, melacak berbagai faktor yang mempengaruhi kinerja, dan menunjukkan jenis intervensi untuk peningkatan kinerja (misalnya, pelatihan, umpan balik). Tujuan dari penelitian ini adalah untuk mendeskripsikan langkah-langkah awal kinerja tim merah dalam rangka meningkatkan kinerja tim merah.

**Penelitian tentang tim dan tim merah**

Penelitian faktor manusia yang ada dalam tim merah sangat terbatas. Analisis tugas kognitif individu dan kelompok peretas yang menyerang jaringan dan situs web telah digunakan untuk mengungkap bagaimana peretas memilih target, mendistribusikan dan berbagi tanggung jawab, dan melakukan serangan sebenarnya (McCloskey & Stanard, 1999). Penelitian eksperimental telah mengukur dampak pertahanan penipuan terhadap serangan terhadap sistem dan jaringan komputer (Cohen, Marin, Sappington, Stewart, & Thomas, 2001). Eksperimen dilakukan atau didanai oleh Badan Proyek Penelitian Lanjutan Pertahanan

(DARPA) menunjukkan penggunaan tim merah dalam mengevaluasi mekanisme pertahanan yang berbeda (Kewley & Bouchard, 2000; Schudel & Wood, 2000b) seperti solusi survivabilitas (Pal, Atighetchi, Webber, Schantz, & Jones, 2003). Eksperimen ini tidak mengevaluasi kinerja tim merah secara langsung, namun telah mengidentifikasi a sejumlah faktor yang dapat berkontribusi terhadap kinerja tim merah, seperti pengalaman atau kemahiran (Pal, et. al, 2003) dan pembelajaran (Kewley & Bouchard, 2000; Pal et al., 2003). Mereka juga telah mengidentifikasi beberapa perilaku tim merah, seperti penggunaan waktu, proses kerja, dan persepsi risiko (Schudel & Wood, 2000b). Penelitian telah dilakukan untuk mengembangkan ukuran faktor kerja lawan atau faktor kerja tim merah (Schudel & Wood, 2000b; Wood & Bouchard, 2001). Faktor kerja tim merah mengukur jumlah upaya yang diperlukan oleh tim merah (musuh) untuk menyelesaikan serangan (yaitu untuk merebut bendera)
(Kayu & Bouchard, 2001). Eksperimen yang dilakukan oleh DARPA menunjukkan bahwa faktor kerja tim merah dapat berguna dalam membandingkan konfigurasi sistem yang berbeda (Schudel & Wood, 2000b), terutama jika kemampuan tim merah berbeda-beda. Kemampuan dapat mencakup perilaku tim merah yang berbeda, yang bergantung pada persiapan, pelatihan, dan bakat mereka. Namun, faktor kerja tim merah mungkin lebih merupakan ukuran kemampuan tim merah dibandingkan perbaikan sistem (Schudel & Wood, 2000b). Faktor kerja tim merah mungkin masih berguna dalam mengukur efektivitas tim merah. Khususnya, ketika dihadapkan pada banyak masalah, membandingkan faktor kerja tim merah antara berbagai latihan yang dilakukan oleh tim yang sama dapat memberikan informasi tentang bagaimana karakteristik tim yang berbeda mempengaruhi faktor kerja tim merah (Wood & Bouchard, 2001). Ketika mencoba mengidentifikasi faktor-faktor yang berkontribusi terhadap kinerja tim merah, faktor kerja tim merah dapat menjadi *salah satu* ukuran kinerja tim merah yang dapat dikorelasikan dengan berbagai karakteristik tim.

Untuk memahami apa yang diperlukan untuk kerja tim yang efektif, pertama-tama kita perlu mendefinisikan sebuah tim. Sebuah tim adalah sekumpulan dua atau lebih individu yang berinteraksi secara saling bergantung dan adaptif menuju tujuan atau sasaran bersama (Cannon-Bowers & Salas, 1998). Ada berbagai jenis tim dan tim merah Sandia paling cocok dengan definisi tim kerja. Tim kerja merupakan unit kerja berkelanjutan yang bertanggung jawab memproduksi barang atau menyediakan jasa, keanggotaan mereka biasanya stabil dan penuh waktu, serta terdefinisi dengan baik (Cohen & Bailey, 1997).
Definisi ini juga mencakup tim kerja yang mengelola diri sendiri dengan anggota yang terlatih dalam berbagai keterampilan yang relevan dengan tugas yang mereka lakukan.

Tidak ada satu pun ukuran kinerja tim yang cocok untuk semua tujuan. Perbedaan dalam penilaian kinerja tim menyangkut hasil versus proses.

Meskipun tim dinilai sebagian besar karena hasil yang mereka peroleh, ukuran-ukuran ini sering kali mengandung perbedaan yang disebabkan oleh faktor-faktor selain kerja tim (Brannick & Prince, 1997). Ukuran proses tim mungkin lebih dekat dengan gambaran sebenarnya dari fungsi tim, namun ukuran kinerja tim yang komprehensif perlu mengandung elemen proses dan hasil (Brannick & Prince, 1997). Jenis utama ukuran kinerja tim adalah: (1) ukuran deskriptif (yaitu proses), yang menggambarkan apa yang terjadi pada waktu tertentu dan berupaya mendokumentasikan perilaku individu dan tim; (2) ukuran evaluatif (yaitu hasil), yang menilai kinerja berdasarkan standar yang dapat diidentifikasi dan berfungsi untuk menjawab pertanyaan tentang efektivitas; dan (3) tindakan diagnostik (yaitu proses), yang berupaya mengidentifikasi penyebab perilaku dan mempertanyakan bagaimana dan mengapa hal-hal terjadi (Paris, Salas, & Cannon-

Bower, 2000). Langkah-langkah diagnostik berkontribusi terhadap masukan pada proses umpan balik yang diperlukan untuk meningkatkan kinerja selanjutnya (Salas & Cannon-Bowers, 1997).

## METODE

Karena kurangnya penelitian mengenai efektivitas tim merah dan sifat eksploratif dari penelitian ini, maka desain penelitian bersifat kualitatif, terdiri dari unsur-unsur berikut: lima belas wawancara individu semi-terstruktur dan dua kelompok fokus dengan anggota tim merah, observasi terhadap a sesi pelatihan kelompok tim merah, kehadiran presentasi teknis Sandia, pengamatan pribadi terhadap lingkungan sekitar lokasi, dan analisis dokumen yang berkaitan dengan kerja tim merah. Data dikumpulkan oleh penulis pertama. Wawancara individu dan kelompok fokus menggunakan panduan wawancara terbuka yang sama. Lihat Lampiran 1 untuk panduan wawancara. Wawancara individu berlangsung sekitar satu jam dan kelompok fokus berlangsung sekitar dua setengah jam. Satu kelompok fokus dan sebelas wawancara direkam dengan audio dan satu kelompok fokus dan empat wawancara individual tidak direkam dengan audio.

Catatan pribadi tentang interaksi ini diambil oleh penulis pertama dan rekaman audionya ditranskrip.

Program IDART terdiri dari anggota tim inti, non inti, dan matriks merah. Anggota inti tim merah adalah analis sistem yang secara teratur berpartisipasi dalam proyek tim merah dan yang pekerjaan penuh waktunya berada di departemen penilaian IDART. Anggota non-inti adalah analis sistem yang berpartisipasi secara semi-reguler dalam proyek tim merah dan bukan anggota departemen penilaian IDART. Anggota Matrix jarang berpartisipasi dalam proyek tim merah. Mereka diakses berdasarkan keahlian spesifik mereka, yang diperlukan untuk sistem spesifik yang sedang dipertimbangkan. Misalnya, tim merah yang memeriksa sistem deteksi agen biologis dan kimia dapat mencakup para ahli di bidang agen perang biologis dan kimia. Anggota-anggota ini diakses dari kumpulan ahli dalam organisasi Sandia. Wawancara individu dilakukan terhadap sebelas anggota inti, tiga anggota non-inti, dan dua anggota matriks. Kelompok fokus pertama terdiri dari enam anggota inti dan kelompok fokus kedua terdiri dari tujuh anggota inti.

Catatan yang ditranskrip dan wawancara dianalisis dengan mengkodekan tema wawancara dan observasi menggunakan paket perangkat lunak kualitatif, QSR NVivo©. Struktur pengkodean terdiri dari node, yang mewakili kategori efektivitas tim merah yang ditentukan. Saat diberi kode, sebuah node menyimpan referensi ke bagian teks dari data observasi dan wawancara. Dalam makalah ini, data analisis kinerja dilaporkan dan dibahas.

## HASIL

Temuan dilaporkan dalam total kategori pengukuran dan dimensi pengukuran yang paling sering dikutip. Proses pengkodean menghasilkan 67 node dan jumlah komentar yang diberi kode sebanyak 95. Node tersebut dikelompokkan menjadi lima kategori besar. Empat kategori pertama ditetapkan ke dalam empat perspektif: (1) anggota tim individu (12 komentar); (2) tim secara keseluruhan (27 komentar); (3) manajemen (12 komentar); dan (4) pelanggan (30 komentar).
Kategori perspektif ini selanjutnya dikelompokkan menjadi tiga dimensi pengukuran tim: deskriptif, evaluatif, dan diagnostik. Lihat Tabel 1 untuk ringkasan jumlah komentar pada kategori perspektif kinerja. Kategori kelima berisi komentar mengenai kesulitan mengukur efektivitas tim merah (14 komentar). Dimensi pengukuran dengan jumlah komentar terbanyak dalam setiap kategori perspektif dilaporkan.

Tabel 1. Komentar mengenai kinerja tim merah

| Jenis Pengukuran \ Perspektif | | | | | |
|---|---|---|---|---|---|
| Deskriptif (Proses) | 0 | 0 | 11 | 22 | **33** |
| Evaluatif (Hasil) | 0 | 14 | 1 | 8 | **23** |
| Diagnostik (Proses) | 12 | 13 | 0 | 0 | **25** |
| **Total** | **12** | **27** | **12** | **30** | **81** |

Ukuran individu anggota tim yang paling sering dikutip adalah diagnostik (12 komentar). Dalam pengelompokan ini, dimensi pengembangan profesional individu (4 komentar) paling sering dilaporkan. Pengembangan profesional individu didefinisikan sebagai pertumbuhan individu dalam ilmu komputer dan kecerdasan analisis sistem. Salah satu anggota inti menggambarkan pengalaman ini: “Khususnya di lingkungan khusus kami di mana kami tidak seperti montir mobil yang dilatih untuk melakukan sesuatu dan setiap kali Anda menyervis mesin. Kita perlu belajar di setiap keterlibatan… sangat penting.”

Dari perspektif tim secara keseluruhan, ukuran efektivitas yang paling sering dikutip adalah evaluatif (14 komentar) dan diagnostik (13 komentar). Pemahaman sistem (5 komentar), dimensi yang paling sering dikutip dalam kategori pengukuran evaluatif tim, didefinisikan sebagai sejauh mana tim merah mensintesis dan mengkarakterisasi sistem dari sudut pandang yang berbeda. Salah satu anggota inti menjelaskan pemahaman sistem: “Pemahaman sistem merupakan hal mendasar yang mengetahui akar penyebab kelemahan sistem. Hal ini lebih dari upaya audit lain yang memindai kerentanan; tim merah melihat perangkat keras, perangkat lunak, tata letak fisik, proses organisasi, dan kebijakan. Tim merah berkomunikasi di seluruh fungsi organisasi pelanggan dan mereka menciptakan pandangan yang bahkan tidak dimiliki oleh organisasi itu sendiri. Tim merah “menggabungkan” elemen-elemen ini ke dalam pemahaman yang lebih besar, yang merupakan sesuatu yang akan dimanfaatkan oleh musuh.” Dinamika tim (10 komentar) adalah dimensi yang paling sering dikutip dalam kategori pengukuran diagnostik tim, dan didefinisikan sebagai perilaku dan sikap tim. Komentar untuk menggambarkan dinamika tim: “Tidak peduli seberapa banyak Anda merencanakan atau mempersiapkan serangan, ada banyak sekali variabel yang berubah ketika Anda beralih dari *persiapan* ke *tindakan.* Ruang ini tidak memiliki perencanaan apa pun, dan di situlah dinamika tim muncul

di dalam." Anggota tim merah menghabiskan banyak waktu dalam tahap perencanaan (yaitu mendeskripsikan sistem, mengidentifikasi kerentanan, merencanakan serangan). Ketika tim berpindah dari fase perencanaan ke melakukan serangan terhadap suatu sistem, waktu terbatas. Dinamika tim yang baik menunjukkan kemampuan tim merah untuk mengatasi dan menyelesaikan masalah tak terencana yang muncul dalam situasi serangan dengan cepat dan akurat.

Pada kategori perspektif manajemen, ukuran yang paling sering dikutip adalah pada dimensi deskriptif. Mendapatkan semua target sistem dalam simulasi serangan (4 komentar) adalah ukuran deskriptif yang paling sering dikutip. Penjelasan mengenai pentingnya target sistem tim merah: “Dalam keterlibatan tim merah, kami sangat berhati-hati dalam menentukan tujuan atau “bendera” apa yang dimaksud. Jika tidak, pada akhirnya, sangat sulit untuk menentukan apakah Anda berhasil atau tidak.”

Dari perspektif pelanggan dalam tim merah, kinerja sebagian besar bersifat deskriptif (22 komentar). Kualitas komunikasi dengan pelanggan (14 komentar) adalah dimensi pengukuran deskriptif pelanggan yang paling sering dikutip. Komunikasi dengan pelanggan berkaitan dengan kemudahan komunikasi (misalnya, aksesibilitas pelanggan ke tim dan sebaliknya), frekuensi komunikasi, formalisme komunikasi, dan umpan balik dari pelanggan yang diperoleh melalui berbagai langkah dalam metodologi penilaian. Komentar untuk menjelaskan sudut pandang komunikasi dan umpan balik pelanggan: “Apakah Anda dapat menunjukkan kepada pelanggan bahwa mereka terlindungi dengan baik atau ada lubang? Ini tergantung bagaimana pelanggan memandang informasi yang Anda berikan dan solusi apa yang Anda berikan kepada mereka.”

Anggota tim merah menyatakan kesulitan dalam mengukur efektivitas tim merah (total 14 komentar). Di antara berbagai topik yang disebutkan, kesulitan dalam mengukur seberapa efektif pekerjaan mereka bagi pelanggan (9 komentar) menjadi topik yang paling banyak disebutkan. Salah satu anggota tim merah berbicara tentang kesulitan dalam menilai efektivitas pekerjaan dari sudut pandang pelanggan: “Karena setiap penilaian yang kami lakukan sangat unik dan berbeda, saya pikir sangat sulit untuk menghasilkan metrik yang dapat Anda gunakan untuk mengukur efektivitas tim merah. Saya pikir itulah yang sebenarnya terjadi, adalah pelanggan. Masalahnya adalah apakah kita telah melakukan pekerjaan dengan baik atau tidak, apakah mereka berpikir kita telah… mengambil upaya yang baik, sungguh.”

## DISKUSI

Studi saat ini berfokus pada mendeskripsikan dimensi ukuran kinerja tim merah. Berbagai perspektif yang dilaporkan oleh anggota tim merah konsisten dengan literatur tim yang menekankan perlunya lebih dari satu jenis pengukuran kinerja (yaitu ukuran proses dan hasil). Secara umum, tim merah menekankan pada perspektif tim dan pelanggan. Pada tingkat kinerja tim, anggota tim merah cenderung melihatnya baik secara diagnostik maupun evaluatif, dan berasumsi bahwa proses tim tidak hanya merupakan ukuran yang penting, namun juga keluaran tim. Dinamika tim menonjol sebagai ukuran penting. Sandia merah tim menghabiskan banyak waktu untuk menilai sistem dan menciptakan 'beberapa tampilan sistem'. Hal ini mencakup brainstorming dan perencanaan serangan, upaya yang memerlukan upaya kelompok yang besar, biasanya di bawah tekanan waktu yang terbatas. Anggota tim merah juga menekankan langkah-langkah evaluatif tim (yaitu hasil). Mereka menyoroti 'pelajaran yang didapat' di akhir proyek sebagai penanda hal-hal yang berjalan baik dalam proyek, serta permasalahan yang dihadapi. Selain itu, sejauh mana tim merah memahami dan secara akurat mengkarakterisasi sistem yang sedang dipertimbangkan juga ditekankan.
Seberapa baik tim menciptakan pemahaman sistem berhubungan langsung dengan ukuran keberhasilan akhir, menangkap tanda-tanda serangan yang direncanakan. Proses pembelajaran atau umpan balik yang ditekankan dalam penelitian ini dapat menjadi ukuran lain untuk diperiksa ketika menilai kinerja tim merah di masa depan.

Anggota tim Merah memandang perspektif kinerja pelanggan sebagian besar bersifat deskriptif, dan menganggap komunikasi dengan pelanggan sebagai ukuran utama. Karena pelanggan tidak hadir dalam semua proses tim di mana dinamika tim atau faktor tim utama lainnya berperan, kualitas interaksi dengan pelanggan penting untuk mengatasi cara kerja tim dan mencapai tujuan proyeknya. Dalam studi tim merah sebelumnya, perspektif pelanggan tidak dibahas. Menilai perspektif tersebut mungkin bermanfaat dalam memvalidasi evaluasi kinerja anggota tim merah.

Anggota tim merah menggambarkan efektivitas masing-masing anggota dalam hal pembelajaran profesional dan kesenangan di tempat kerja. Pembelajaran individu selama proyek dianggap sebagai ukuran efektivitas yang penting karena keunikan setiap proyek. Dimensi pengukuran kinerja masing-masing anggota tim ini mungkin berguna dalam melacak bagaimana peningkatan pembelajaran profesional berkorelasi dengan ukuran hasil lainnya, seperti meraih tanda atau mencapai pernyataan tujuan kerja lainnya (misalnya, keterbatasan waktu dan anggaran).

Singkatnya, anggota tim merah menjelaskan berbagai ukuran efektivitas tim merah. Hal ini berkisar dari perilaku dan sikap tim hingga tindakan yang lebih mudah diukur seperti memenuhi tenggat waktu dan mencapai target sistem. Dalam studi tim merah sebelumnya (Schudel & Wood, 2000b; Wood & Bouchard, 2001) waktu untuk menyelesaikan suatu penugasan, seperti faktor kerja tim merah, membahas ukuran terukur yang dapat digunakan untuk mengukur beberapa dimensi kinerja tim merah. Berbagai ukuran yang dibahas dalam penelitian ini dapat memperluas pemahaman tentang kinerja tim merah karena faktor-faktor lain yang mempengaruhi kinerja dapat digunakan untuk perbaikan sistem yang sedang diperiksa serta kinerja tim merah.

## KESIMPULAN

Pengukuran efektivitas tim merah yang komprehensif dapat meningkatkan kinerja tim merah dalam beberapa cara. Pertama, untuk menentukan efektivitas tim merah guna menunjukkan dengan tepat kekuatan dan kelemahan kinerja tim, harus ada serangkaian ukuran kinerja tim. Kedua, tim berkembang seiring waktu (Morgan, Glickman, Woodard, Blaiwes, &

Salas, 1986) dan lamanya waktu mereka bekerja sama dapat mempunyai pengaruh yang signifikan terhadap proses kelompok (Foushee, Lauber, Baetge, & Acomb, 1986). Menetapkan pengukuran dasar dan berkelanjutan terhadap kinerja tim merah dapat memberikan umpan balik dan mekanisme lain untuk koreksi diri seiring berjalannya waktu. Hal ini memiliki implikasi yang signifikan bagi tim kerja yang dikelola sendiri (Cannon-Bowers & Salas, 1998) dan mungkin juga diterapkan pada tim merah Sandia. Lebih lanjut, eksperimen tim merah, seperti mengukur faktor kerja tim merah, memerlukan penetapan dasar untuk tim merah dan kinerja sistem sebelum melakukan beberapa kali percobaan tertentu (Schudel & Wood, 2000b). Ketiga, serangkaian ukuran kinerja akan membantu memandu upaya perbaikan tim, seperti pelatihan tim atau alokasi sumber daya.

Keterbatasan penelitian ini mencakup fakta bahwa deskripsi tindakan hanya didasarkan pada persepsi anggota tim merah. Selanjutnya, tim merah IDART mewakili *salah satu* jenis tim merah. Ada tim merah lain yang ada dan akan menarik untuk menilai apakah dimensi kinerja yang sama atau berbeda akan diidentifikasi di grup lain. Hal ini termasuk memperluas pekerjaan awal ini dengan mewawancarai anggota dan pemimpin tim merah lainnya di Sandia, serta tim merah lainnya. Bidang pekerjaan lain di masa depan adalah penyelidikan faktor-faktor yang berkontribusi dan menghambat kinerja tim merah. Selain mewawancarai anggota tim merah, kami dapat melakukan pengamatan interaksi tim merah pada tahapan berikut: pembentukan tim, sesi curah pendapat, sesi perumusan kerentanan dan serangan kandidat, keterlibatan sistem, dan sesi penutupan. Mengidentifikasi faktor-faktor ini, seperti desain tim atau komposisi anggota, dapat membantu menentukan cara mengonfigurasi tim merah yang berkinerja tinggi. Ada banyak hal yang harus dipelajari tentang faktor-faktor yang terkait dengan kinerja tim merah dan memahami pengukuran kinerja tim merah dan berbagai aspeknya adalah langkah pertama dalam penyelidikan ini.

## UCAPAN TERIMA KASIH

Pendanaan yang disediakan oleh Departemen Pertahanan untuk "Pemodelan dan Simulasi Perlindungan Infrastruktur Kritis" (#DAAD19-01-1-0502, PI: S.Robinson, UW-Madison).

## REFERENSI

Brannick, MT, & Pangeran, C. (1997). Ikhtisar pengukuran kinerja tim. Dalam MT Brannick & E. Salas & C. Prince (Eds.), *Penilaian dan Pengukuran Kinerja Tim* (hlm. 3-16). Mahwah, NJ: Rekan Lawrence Erlbaum.

Meriam-Bowers, JA, & Salas, E. (1998). Kinerja tim dan pelatihan di lingkungan yang kompleks: Temuan terbaru dari penelitian terapan. *Arah Saat Ini dalam Ilmu Psikologi,* 7(3), 83-87.

Carayon, P., Duggan, R., & Kraemer, S. (2003). Sebuah model kinerja tim merah. Dalam KJ Zink (Ed.), *Simposium Internasional Ketujuh tentang Faktor Manusia dalam Desain dan Manajemen Organisasi.* Aachen, Jerman.

Cohen, F., Marin, I., Sappington, J., Stewart, C., & Thomas, E. (2001). Eksperimen tim merah dengan teknologi penipuan. *Diperoleh dari Situs Web Intelijen Keamanan Strategis: http:// www.all.net/ journal/ deception/ experiments/ experiments.html.*

Cohen, SG, & Bailey, DE (1997). Apa yang membuat tim bekerja: Riset efektivitas kelompok dari tingkat awal hingga ruang eksekutif. *Jurnal Manajemen,* 23(3), 239-290.

Dewan Riset Nasional Badan Ilmu Komputer dan Telekomunikasi. (2002). *Keamanan Siber Saat Ini dan Besok: Bayar Sekarang atau Bayar Nanti.* Washington, DC: Pers Akademi Nasional.

Satgas Dewan Ilmu Pertahanan. (2003). *Peran dan status kegiatan tim merah Departemen Pertahanan.* Washington, DC: Kantor Wakil Menteri Pertahanan untuk Akuisisi, Teknologi, dan Logistik.

Foushee, HC, Lauber, J., Baetge, M., & Acomb, D. (1986). *Faktor awak kapal dalam operasional penerbangan: III. Signifikansi operasional dari paparan operasi transportasi udara jarak pendek* (NASA Technical Memorandum 88322). Sunnyvale, CA: Pusat Penelitian Badan Penerbangan dan Antariksa Nasional-Ames.

Kewley, DL, & Bouchard, JF (2000). Ringkasan eksperimen pertahanan dinamis program Jaminan Informasi DARPA, *Prosiding Lokakarya IEEE 2000 tentang Jaminan dan Keamanan Informasi* (hlm. 117-122). Akademi Militer Amerika Serikat, West Point, NW.

Lynn, GS, & Reilly, RR (2000). Mengukur kinerja tim. *Manajemen Teknologi Riset,* 43(2), 48-56.

McCloskey, MJ, & Stanard, T. (1999). Analisis tim merah dari medan perang elektronik: Pendekatan kognitif untuk memahami bagaimana peretas bekerja dalam kelompok, *Proceedings of the Human Factors and Ergonomics Society Pertemuan Tahunan ke-43* (hlm. 179-183): Human Factors and Ergonomics Society.

Morgan, BB, Glickman, AS, Woodard, EA, Blaiwes, AS, & Salas, E. (1986). *Pengukuran perilaku tim di lingkungan Angkatan Laut* (Rep. Teknologi No TR-86-014). Orlando, FL: Pusat Pelatihan Angkatan Laut.

Sobat, P., Atighetchi, M., Webber, F., Schantz, R., & Jones, C. (2003). Refleksi dalam mengevaluasi survivabilitas: Eksperimen APOD, *Simposium Internasional IEEE ke-2 tentang Komputasi dan Aplikasi Jaringan (NCA-03).* Royal Sonesta Hotel, Cambridge, MA.

Palmer, CC (2001). Peretasan etis. *Jurnal Sistem IBM,* 40(3), 769-780.

Paris, CR, Salas, E., & Cannon-Bowers, JA (2000). Kerja tim dalam sistem multi-orang: Tinjauan dan analisis. *Ergonomi,* 43(8), 1052-1075.

Salas, E., & Meriam-Bowers, JA (1997). Metode, alat, dan strategi untuk pelatihan tim. Dalam MA Quinones & A. Ehrenstein (Eds.), *Pelatihan untuk Tenaga Kerja yang Berubah dengan Cepat: Penerapan Penelitian Psikologis* (hlm. 249-279). Washington, DC: Asosiasi Psikologi Amerika.

Schudel, G., & Kayu, B. (2000a). Memodelkan perilaku teroris dunia maya, *Prosiding Konferensi: Penelitian tentang Mitigasi Ancaman Orang Dalam terhadap Sistem Informasi-#2.* Santa Monica, California: Rand.

Schudel, G., & Kayu, B. (2000b). Faktor kerja musuh sebagai metrik jaminan informasi, *Prosiding Paradigma Baru dalam Lokakarya Keamanan.* Ballycotton, County Cork, Irlandia: Asosiasi Mesin Komputer.

Tinnel, LS, Saydjari, OS, & Farrell, D. (2002). Strategi dan taktik perang siber: Analisis tujuan, strategi, taktik, dan teknik siber, *Prosiding IEEE 2002: Lokakarya Jaminan Informasi.* Akademi Militer Amerika Serikat, West Point, NY.

Kayu, BJ, & Duggan, R. (1999). Tim merah konsep jaminan informasi tingkat lanjut, *DISCEX2000 DARPA Information Survivability Conference* (hal. SAND99-2590C). Hilton Head, Carolina Selatan.

Kayu, B., & Bouchard, JF (2001). Faktor Kerja Tim Merah Sebagai Pengukuran Keamanan, *Prosiding Lokakarya Scoring dan Pemeringkatan Keamanan Informasi.* Williamsburg, Virginia: Rekan Keamanan Komputer Terapan.

## LAMPIRAN 1

Panduan wawancara individu dan kelompok terfokus 1. Berbagai faktor mempengaruhi kinerja tim merah dan kinerja tim merah dapat dievaluasi pada dimensi yang berbeda. Apa saja kriteria penilaian kinerja tim merah?